

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 [1]

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 James Hall from Glyn Davies. Subject: Anthony Lake Security Certification. [partial] (1 page)	04/22/1997	P6/b(6)
001b. draft	For James Hall from Glyn Davies. Subject: Anthony Lake Security Certification. [partial] (1 page)	04/22/1997	P6/b(6)
002. memo	For Samuel Berger from James Baker and Mary McCarthy. Subject: Defense Adjudication. (5 pages)	07/08/1998	P6/b(6)
003. email	From Karl Hoffman to Various. Subject: Short Notice Vetting. (2 pages)	06/10/1998	P1/b(1)

COLLECTION:

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

FOLDER TITLE:

Personnel Security [1]

2006-1066-F

vz870

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]

FAX TRANSMITTAL / MESSAGE SHEET

TO:	(Organization, Name, Office Telephone, as needed)	
	Chuck Allen	
RECEIVING FAX NUMBER:		202-456-9110
DATE TRANSMITTED:		31 March 1998
ORIGINATING FAX NUMBER →		703-874-3208
ORIGINATOR: James Archibald		
SUBJECT:		
NUMBER OF PAGES → 12 (Including This Sheet)		
MESSAGE / REMARKS 3/31/98 Jannie - this is James Archibald's fax or SPB issue, per my email. - Chuck		

approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity). The agency believes that the final rule is consistent with regulatory philosophy and principles identified in the Executive Order. In addition, the final rule is not a significant regulatory action as defined by the Executive Order and so is not subject to review under the Executive Order.

The Regulatory Flexibility Act requires agencies to analyze regulatory options that would minimize any significant impact of a rule on small entities. Because the final rule involves a minor procedural change that primarily affects FDA and has no direct effect on small companies, the agency certifies that the final rule will not have a significant economic impact on a substantial number of small entities. Therefore, under the Regulatory Flexibility Act, no further analysis is required.

V. Paperwork Reduction Act of 1995

This final rule contains no additional information collection requirements which are subject to review by the Office of Management and Budget under the Paperwork Reduction Act of 1995 (Pub. L. 104-13).

List of Subjects in 21 CFR Part 814

Administrative practice and procedure, Confidential business information, Medical devices, Medical research, Reporting and recordkeeping requirements.

Therefore, under the Federal Food, Drug, and Cosmetic Act and under authority delegated to the Commissioner of Food and Drugs, 21 CFR part 814 is amended as follows:

PART 814—PREMARKET APPROVAL OF MEDICAL DEVICES

1. The authority citation for 21 CFR part 814 continues to read as follows:

Authority: 21 U.S.C. 351, 352, 353, 360, 360c-360j, 371, 372, 373, 374, 375, 379, 379e, 381.

2. Section 814.44 is amended by revising paragraph (d) to read as follows:

§ 814.44 Procedures for review of a PMA.

(d)(1) FDA will issue to the applicant an order approving a PMA if none of the reasons in § 814.45 for denying approval of the application applies. FDA will approve an application on the basis of draft final labeling if the only deficiencies in the application concern editorial or similar minor deficiencies in

the draft final labeling. Such approval will be conditioned upon the applicant incorporating the specified labeling changes exactly as directed and upon the applicant submitting to FDA a copy of the final printed labeling before marketing. FDA will also give the public notice of the order, including notice of and opportunity for any interested persons to request review under section 515(d)(3) of the act. The notice of approval will be placed on FDA's home page on the Internet (<http://www.fda.gov>), and it will state that a detailed summary of information respecting the safety and effectiveness of the device, which was the basis for the order approving the PMA, including information about any adverse effects of the device on health, is available on the Internet and has been placed on public display, and that copies are available upon request. FDA will publish in the Federal Register after each quarter a list of the approvals announced in that quarter. When a notice of approval is published, data and information in the PMA file will be available for public disclosure in accordance with § 814.9.

(2) A request for copies of the current PMA approvals and denials document and for copies of summaries of safety and effectiveness shall be sent in writing to the Dockets Management Branch (HFA-305), Food and Drug Administration, 12420 Parklawn Dr., rm. 1-23, Rockville, MD 20857.

3. Section 814.45 is amended by revising paragraph (d) to read as follows:

§ 814.45 Denial of approval of a PMA.

(d)(1) FDA will give the public notice of an order denying approval of the PMA. The notice will be placed on the FDA's home page on the Internet (<http://www.fda.gov>), and it will state that a detailed summary of information respecting the safety and effectiveness of the device, including information about any adverse effects of the device on health, is available on the Internet and has been placed on public display and that copies are available upon request. FDA will publish in the Federal Register after each quarter a list of the denials announced in that quarter. When a notice of denial of approval is made publicly available, data and information in the PMA file will be available for public disclosure in accordance with § 814.9.

(2) A request for copies of the current PMA approvals and denials document and copies of summaries of safety and effectiveness shall be sent in writing to the Freedom of Information Staff (HFI-

35), Food and Drug Administration, 5600 Fishers Lane, Rockville, MD 20857.

Dated: January 22, 1998.

William B. Schultz,

Deputy Commissioner for Policy.

[FR Doc. 98-2263 Filed 1-29-98; 8:45 am]

BILLING CODE 4160-01-F

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 147

RIN 0790-AG54

Personnel Security Policies for Granting Access to Classified Information

AGENCY: Department of Defense.
ACTION: Interim final rule.

SUMMARY: This rule is published to streamline security practices throughout the government, uniform adjudicative guidelines, investigative standards and guidelines for temporary access are being established. This initiative will simplify security processing and allow the deserving public to obtain a security clearance in a faster, more efficient manner.

DATES: This rule is effective March 24, 1997. Comments must be received by March 31, 1998.

ADDRESSES: Forward comments to the Security Policy Board Staff, 1215 Jefferson Davis Highway, Suite 1101, Arlington, VA 22202.

FOR FURTHER INFORMATION CONTACT: Mr. T. Thompson, 703-602-9969.

SUPPLEMENTARY INFORMATION:

Executive Order 12866, Regulatory Planning and Review

It has been determined that this interim rule (32 CFR part 147) is not a significant regulatory action. The rule does not:

(1) Have an annual effect to the economy of \$100 million or more or adversely affect in a material way the economy; a section of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities;

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency;

(3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive Order.

Public Law 96-354, Regulatory Flexibility Act (5 U.S.C. 601)

It has been certified that this rule is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities. This part will streamline personnel security clearance procedures and make the process more efficient.

Public Law 96-511, Paperwork Reduction Act (44 U.S.C. Chapter 35)

It has been certified that this part does not impose any reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995.

List of Subjects in 32 CFR Part 147

Classified information, Investigations, Security measures.

Accordingly, Title 32 of the Code of Federal Regulations, Chapter I, subchapter C is amended to add part 147 to read as follows:

PART 147—ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION

Subpart A—Adjudicative Guidelines

Sec.

- 147.1 Introduction.
- 147.2 Adjudicative process.
- 147.3 Guideline A—Allegiance to the United States.
- 147.4 Guideline B—Foreign influence.
- 147.5 Guideline C—Foreign preference.
- 147.6 Guideline D—Sexual behavior.
- 147.7 Guideline E—Personal conduct.
- 147.8 Guideline F—Financial considerations.
- 147.9 Guideline G—Alcohol consumption.
- 147.10 Guideline H—Drug involvement.
- 147.11 Guideline I—Emotional, mental, and personality disorders.
- 147.12 Guideline J—Criminal conduct.
- 147.13 Guideline K—Security violations.
- 147.14 Guideline L—Outside activities.
- 147.15 Guideline M—Misuse of information technology systems.

Subpart B—Investigative Standards

- 147.18 Introduction.
- 147.19 The three standards.
- 147.20 Exception to periods of coverage.
- 147.21 Expanding investigations.
- 147.22 Transferability.
- 147.23 Breaks in service.
- 147.24 The national agency check.

Subpart C—Guidelines for Temporary Access

- 147.28 Introduction.
- 147.29 Temporary eligibility for access.

147.30 Temporary eligibility for access at the CONFIDENTIAL AND SECRET levels and temporary eligibility for "L" access authorization.

147.31 Temporary eligibility for access at the TOP SECRET levels and temporary eligibility for "Q" access authorization. For someone who is the subject of a favorable investigation not meeting the investigative standards for access at those levels.

147.32 Temporary eligibility for access at the TOP SECRET and SCI levels and temporary eligibility for "Q" access authorization. For someone who is not the subject of a current, favorable personnel or personnel-security investigation of any kind.

147.33 Additional requirements by agencies.

Authority: E.O. 12968 (60 FR 40245, 3 CFR 1995 Comp., p. 391).

Subpart A—Adjudication

§ 147.1 Introduction.

The following adjudicative guidelines are established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs and are to be used by government departments and agencies in all final clearance determinations.

§ 147.2 Adjudicative process.

(a) The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following actors:

- (1) The nature, extent, and seriousness of the conduct;
- (2) The circumstances surrounding the conduct, to include knowledgeable participation;
- (3) The frequency and recency of the conduct;
- (4) The individual's age and maturity at the time of the conduct;

(5) The voluntariness of participation;

(6) The presence or absence of rehabilitation and other pertinent behavioral changes;

- (7) The motivation for the conduct;
- (8) The potential for pressure, coercion, exploitation, or duress;
- (9) The likelihood of continuation of recurrence.

(b) Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

(c) The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person, as explained further below:

- (1) Guideline A: Allegiance to the United States.
- (2) Guideline B: Foreign influence.
- (3) Guideline C: Foreign preference.
- (4) Guideline D: Sexual behavior.
- (5) Guideline E: Personal conduct.
- (6) Guideline F: Financial considerations.
- (7) Guideline G: Alcohol consumption.
- (8) Guideline H: Drug involvement.
- (9) Guideline I: Emotional, mental, and personality disorders.
- (10) Guideline J: Criminal conduct.
- (11) Guideline K: Security violations.
- (12) Guideline L: Outside activities.
- (13) Guideline M: Misuse of Information Technology Systems.

(d) Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding, the whole person concept, pursuit of further investigations may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

(e) When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

- (1) Voluntarily reported the information;
- (2) Was truthful and complete in responding to questions;

(3) Sought assistance and followed professional guidance, where appropriate;

(4) Resolved or appears likely to favorably resolve the security concern;

(5) Has demonstrated positive changes in behavior and employment;

(6) Should have his or her access temporarily suspended pending final adjudication of the information.

(f) If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

§ 147.3 Guideline A—Allegiance to the United States.

(a) *The concern.* An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;

(2) Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

(3) Association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any state or subdivision, by force or violence or by other unconstitutional means;

(4) Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

(c) *Conditions that could mitigate security concerns include:* (1) The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

(2) The individual's involvement was only with the lawful or humanitarian aspects of such an organization;

(3) Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;

(4) The person has had no recent involvement or association with such activities.

§ 147.4 Guideline B—Foreign Influence.

(a) *The concern.* A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom he or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

(2) Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;

(3) Relatives, cohabitants, or associates who are connected with any foreign government;

(4) Failing to report, where required, associations with foreign nationals;

(5) Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;

(6) Conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;

(7) Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;

(8) A substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

(c) *Conditions that could mitigate security concerns include:* (1) A determination that the immediate family member(s) (spouse, father, mother, sons, daughters, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States;

(2) Contacts with foreign citizens are the result of official United States Government business;

(3) Contact and correspondence with foreign citizens are casual and infrequent;

(4) The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country;

(5) Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

§ 147.5 Guideline C—Foreign preference.

(a) *The concern.* When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

(b) *Conditions that could raise a security concern and may be disqualifying include:*

(1) The exercise of dual citizenship;

(2) Possession and/or use of a foreign passport;

(3) Military service or a willingness to bear arms for a foreign country;

(4) Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;

(5) Residence in a foreign country to meet citizenship requirements;

(6) Using foreign citizenship to protect financial or business interests in another country;

(7) Seeking or holding political office in the foreign country;

(8) Voting in foreign elections;

(9) Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

(c) *Conditions that could mitigate security concerns include:* (1) Dual citizenship is based solely on parents' citizenship or birth in a foreign country;

(2) Indicators of possible foreign preference (e.g., foreign military service occurred before obtaining United States citizenship);

(3) Activity is sanctioned by the United States;

(4) Individual has expressed a willingness to renounce dual citizenship.

§ 147.6 Guidance D—Sexual behavior.

(a) *The concern.* Sexual behavior is security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, duress, or reflects lack of judgment or discretion.¹ Sexual orientation or

¹ The adjudicator should also consider guidance pertaining to criminal conduct (Guideline J) and

with preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(2) Compulsive or addictive sexual behavior when the person is unable to stop a pattern or self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;

(3) Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

(4) Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

(c) *Conditions that could mitigate security concerns include:* (1) The behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;

(2) The behavior was not recent and there is no evidence of subsequent conduct of a similar nature;

(3) There is no other evidence of questionable judgment, irresponsibility, or emotional instability;

(4) The behavior no longer serves as a basis for coercion, exploitation, or duress.

§ 147.7 Guideline E—Personal conduct.

(a) *The concern.* Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(1) Refusal to undergo or cooperate with required security processing, including medical and psychological testing;

(2) Refusal to complete required security forms, releases, or provide full, frank and truthful answers to lawful questions of investigators, security officials or other representatives in connection with a personnel security or trustworthiness determination.

(b) *Conditions that could raise a security concern and may be disqualifying also include:* (1) Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

emotional, mental and personality disorders (Guideline I) in determining how to resolve the security concerns raised by sexual behavior.

(2) The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(3) Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other representative in connection with a personnel security or trustworthiness determination;

(4) Personal conduct or concealment of information that may increase an individual's vulnerability to coercion, exploitation, or duties, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;

(5) A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency;

(6) Association with persons involved in criminal activity.

(c) *Conditions that could mitigate security concerns include:* (1) The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

(2) The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

(3) The individual made prompt, good faith efforts to correct the falsification before being confronted with the facts;

(4) Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

(5) The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;

(6) A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information;

(7) Association with persons involved in criminal activities has ceased.

§ 147.8 Guideline F—Financial considerations.

(a) *The concern.* An individual who is financially overextended is at risk of

having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) A history of not meeting financial obligations;

(2) Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

(3) Inability or unwillingness to satisfy debts;

(4) Unexplained affluence;

(5) Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

(c) *Conditions that could mitigate security concerns include:* (1) The behavior was not recent;

(2) It was an isolated incident;

(3) The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);

(4) The person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;

(5) The affluence resulted from a legal source;

(6) The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

§ 147.9 Guideline G—Alcohol consumption.

(a) *The concern.* Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;

(2) Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;

(3) Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

(4) Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff

member of a recognized alcohol treatment program;

(5) Habitual or binge consumption of alcohol to the point of impaired judgment;

(6) Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program.

(c) *Conditions that could mitigate security concerns include:* (1) The alcohol related incidents do not indicate a pattern;

(2) The problem occurred a number of years ago and there is no indication of a recent problem;

(3) Positive changes in behavior supportive of sobriety;

(4) Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, has abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

§ 174.10 Guideline H—Drug involvement.

(a) *The concern.* (1) Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

(2) Drugs are defined as mood and behavior altering substances, and include:

(i) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens).

(ii) Inhalants and other similar substances.

(3) Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Any drug abuse (see above definition);

(2) Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;

(3) Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

(4) Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

(5) Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional. Recent drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will almost invariably result in an unfavorable determination.

(c) *Conditions that could mitigate security concerns include:* (1) The drug involvement was not recent;

(2) The drug involvement was an isolated or aberration event;

(3) A demonstrated intent not to abuse any drugs in the future;

(4) Satisfactory completion of a prescribed drug treatment program, including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.

§ 147.11 Guideline I—Emotional, mental, and personality disorders.

(a) *The concern:* Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupation functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability, or stability. A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to or approved by the government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) An opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;

(2) Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication;

(3) A pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;

(4) Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

(c) *Conditions that could mitigate security concerns include:* (1) There is no indication of a current problem;

(2) Recent opinion by a credentialed mental health professional that an

individual's previous emotional, mental, or personality disorder is cured, under control or in remission and has a low probability of recurrence or exacerbation;

(3) The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

§ 147.12 Guideline J—Criminal conduct.

(a) *The concern.* A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Allegations or admissions of criminal conduct, regardless of whether the person was formally charged;

(2) A single serious crime or multiple lesser offenses.

(c) *Conditions that could mitigate security concerns include:* (1) The criminal behavior was not recent;

(2) The crime was an isolated incident;

(3) The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;

(4) The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;

(5) Acquittal;

(6) There is clear evidence of successful rehabilitation.

§ 147.13 Guideline K—Security violations.

(a) *The concern.* Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Unauthorized disclosure of classified information;

(2) Violations that are deliberate or multiple or due to negligence.

(c) *Conditions that could mitigate security concerns include actions that:*

(1) Were inadvertent;

(2) Were isolated or infrequent;

(3) Were due to improper or inadequate training;

(4) Demonstrate a positive attitude towards the discharge of security responsibilities.

§ 147.14 Guideline L—Outside activities.

(a) *The concern.* Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's

security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

(b) *Conditions that could raise a security concern and may be disqualifying include any service, whether compensated, volunteer, or employment with:* (1) A foreign country;

(2) Any foreign national;

(3) A representative of any foreign interest;

(4) Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

(c) *Conditions that could mitigate security concerns include:* (1) Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;

(2) The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

§ 147.15 Guideline M—Misuse of information technology systems.

(a) *The concern.* Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Illegal or unauthorized entry into any information technology system;

(2) Illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system;

(3) Removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

(4) Introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

(c) *Conditions that could mitigate security concerns include:* (1) The misuse was not recent or significant;

(2) The conduct was unintentional or inadvertent;

(3) The introduction or removal of media was authorized;

(4) The misuse was an isolated event;

(5) The misuse was followed by a prompt, good faith effort to correct the situation.

Subpart B—Investigative Standards

§ 147.18 Introduction.

The following investigative standards are established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information and Special Access Programs, and are to be used by government departments and agencies as the investigative basis for final clearance determinations. However, nothing in these standards prohibits an agency from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

§ 147.19 The three standards.

There are three standards (Attachment D to this subpart part summarizes when to use each one):

(a) The investigation and reinvestigation standards for "L" access authorizations and for access to confidential and secret (including all secret-level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by section in 4.4 of Executive Order 12958) (60 FR 19825, 3 CFR 1995 Comp., p. 33);

(b) The investigation standard for "Q" access authorizations and for access to top secret (including top secret Special Access Programs) and Sensitive Compartmented Information;

(c) The reinvestigation standard for continued access to the levels listed in paragraph (b) of this section.

§ 147.20 Exception to periods of coverage.

Some elements of standards specify a period of coverage (e.g. seven years). Where appropriate, such coverage may be shortened to the period from the subject's eighteenth birthday to the present or to two years, whichever is longer.

§ 147.21 Expanding investigations.

Investigations and reinvestigations may be expanded under the provisions

of Executive Order 12968 (60 FR 40245, 3 CFR 1995 Comp., p. 391) and other applicable statutes and Executive Orders.

§ 147.22 Transferability.

Investigations that satisfy the requirements of a given standard and are current meet the investigative requirements for all levels specified for the standard. They shall be mutually and reciprocally accepted by all agencies.

§ 147.23 Breaks in service.

If a person who requires access has been retired or separated from U.S. government employment for less than two years and is the subject of an investigation that is otherwise current, the agency regranting the access will, as a minimum, review an updated Standard Form 86 and applicable records. A reinvestigation is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968 (60 FR 40245, 3 CFR 1995 Comp., p. 391); (Attachment D to this subpart, Table 2).

§ 147.24 The national agency check.

The National Agency Check is a part of all investigations and reinvestigations. It consists of a review of:

(a) Investigative and criminal history files of the FBI, including a technical fingerprint search;

(b) OPM's Security/Suitability Investigations Index;

(c) DoD's Defense Clearance and Investigations Index;

(d) Such other national agencies (e.g., CIA, INS) as appropriate to the individual's background.

Attachment A to Subpart B—Standard A—National Agency Check With Local Agency Checks and Credit Check (NACLC)

(a) *Applicability.* Standard A applies to investigations and reinvestigations for:

(1) Access to CONFIDENTIAL and SECRET (including all SECRET-level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by sect. 4.4 of Executive Order 12958) (60 FR 19825, 3 CFR 1995 Comp., p. 333);

(2) "L" access authorizations;

(b) *For Reinvestigation: When to Reinvestigate.* The reinvestigation may be initiated at any time following completion of, but not later than ten years (fifteen years for CONFIDENTIAL) from the date of, the previous investigation or reinvestigation. (Attachment D to this subpart, Table 2, reflects the specific requirements for when to request a reinvestigation, including when there has been a break in service.)

(c) *Investigative Requirements.*

Investigative requirements are as follows:

(1) *Completion of Forms*: Completion of Standard Form 86, including applicable releases and supporting documentation.

(2) *National Agency Check*: Completion of a National Agency Check.

(3) *Financial Review*: Verification of the subject's financial status, including credit bureau checks covering all locations where the subject has resided, been employed, or attended school for six months or more for the past seven years.

(4) *Date and Place of Birth*: Corroboration of date and place of birth through a check of appropriate documentation, if not completed in any previous investigation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

(5) *Local Agency Checks*: As a minimum, all investigations will include checks of law enforcement agencies having jurisdiction where the subject has lived, worked, and/or attended school within the last five years, and, if applicable, of the appropriate agency for any identified arrests.

(d) *Expanding the Investigation*: The investigation may be expanded if necessary to determine if access is clearly consistent with the national security.

Attachment B to Subpart B—Standard B—Single Scope Background Investigation (SSBI)

(a) *Applicability*. Standard B applies to initial investigations for:

(1) Access to TOP SECRET (including TOP SECRET Special Access Programs) and Sensitive Compartment Information;

(2) "Q" access authorizations.

(b) *Investigative Requirements*. Investigative requirements are as follows:

(1) *Completion of Forms*: Completion of Standard Form 86, including applicable releases and supporting documentation.

(2) *National Agency Check*: Completion of a National Agency Check.

(3) *National Agency Check for the Spouse or Cohabitant (if applicable)*: Completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant.

(4) *Date and Place of Birth*: Corroboration of date and place of birth through a check of appropriate documentation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

(5) *Citizenship*: For individuals born outside the United States, verification of US citizenship directly from the appropriate registration authority; verification of US citizenship or legal status of foreign-born immediate family members (spouse, cohabitant, father, mother, sons, daughters, brothers, sisters).

(6) *Education*: Corroboration of most recent or most significant claimed attendance, degree, or diploma. Interviews of appropriate educational sources if education is a primary activity of the subject during the most recent three years.

(7) *Employment*: Verification of all employments for the past seven years; personal interviews of sources (supervisors, coworkers, or both) for each employment of six months or more; corroboration through records or sources of all periods of unemployment exceeding sixty days; verification of all prior federal and military

service, including discharge type. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

(8) *References*: Four references, of whom at least two are developed; to the extent practicable, all should have social knowledge of the subject and collectively span at least the last seven years.

(9) *Former Spouse*: An interview of any former spouse divorced within the last ten years.

(10) *Neighborhoods*: Confirmation of all residences for the last three years through appropriate interviews with neighbors and through records reviews.

(11) *Financial Review*: Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the last seven years.

(12) *Local Agency Checks*: A check of appropriate criminal history records covering all locations where, for the last ten years, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.

Note: If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.

(13) *Public Records*: Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject.

(14) *Subject Interview*: A subject interview, conducted by trained security, investigative, or counterintelligence personnel. During the investigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

(15) *Polygraph (only in agencies with approved personnel security polygraph programs)*: In departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, the investigation may include a polygraph examination, conducted by a qualified polygraph examiner.

(c) *Expanding the Investigation*. The investigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

Attachment C to Subpart B—Standard C—Single Scope Background Investigation Periodic Reinvestigation (SSBI-PR)

(a) *Applicability*. Standard C applies to reinvestigation for:

(1) Access to TOP SECRET (including TOP SECRET Special Access Programs) and Sensitive Compartmented Information;

(2) "Q" access authorizations.

(b) *When to Reinvestigate*. The reinvestigation may be initiated at any time following completion of, but not later than

five years from the date of, the previous investigation (see Attachment D to this subpart, Table 2).

(c) *Reinvestigative Requirements*.

Reinvestigative requirements are as follows:

(1) *Completion of Forms*: Completion of Standard Form 86, including applicable releases and supporting documentation.

(2) *National Agency Check*: Completion of a National Agency Check (fingerprint cards are required only if there has not been a previous valid technical check of the FBI).

(3) *National Agency Check for the Spouse or Cohabitant (if applicable)*: Completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant. The National Agency Check for the spouse or cohabitant is not required if already completed in conjunction with a previous investigation or reinvestigation.

(4) *Employment*: Verification of all employments since the last investigation. Attempts to interview a sufficient number of sources (supervisors, coworkers, or both) at all employments of six months or more. For military members, all services within one branch of the armed forces will be considered as one employment, regardless of assignments.

(5) *References*: Interviews with two character references who are knowledgeable of the subject; at least one will be a developed reference. To the extent practical, both should have social knowledge of the subject and collectively span the entire period of the reinvestigation. As appropriate, additional interviews may be conducted, including with cohabitants and relatives.

(6) *Neighborhoods*: Interviews of two neighbors in the vicinity of the subject's most recent residence of six months or more. Confirmation of current residence regardless of length.

(7) *Financial Review—Financial Status*: Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the period covered by the reinvestigation.

(ii) *Check of Treasury's Financial Data Base*: Agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, and transactions under \$10,000 that are reported as possible money laundering violations.

(8) *Local Agency Checks*: A check of appropriate criminal history records covering all locations where, during the period covered by the reinvestigation, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. (Note: If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.)

(9) *Former Spouse*: An interview with any former spouse unless the divorce took place before the date of the last investigation or reinvestigation.

(10) **Public Records:** Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject since the date of the last investigation.

(11) **Subject Interview:** A subject interview, conducted by trained security, investigative, or counterintelligence personnel. During the

reinvestigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

(d) **Expanding the Reinvestigation:** The reinvestigation may be expanded as

necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

Attachment D to Subpart B—Decision Tables

TABLE 1.—WHICH INVESTIGATION TO REQUEST

If the requirement is for	And the person has this access	Based on this investigation	Then the investigation required is	Using standard
Confidential Secret; "L"	None	None Out of date NACLC or SSBI.	NACLC	A
Top Secret, SCI; "Q"	Conf, Sec; "L" None None; Conf, Sec; "L"	None Current or out of date NACLC Out of date SSBI	SSBI	B
	TS, SCI; "Q"		SSBI-PR	C

TABLE 2.—REINVESTIGATION REQUIREMENTS

If the requirement is for	And the age of the investigation is	Type required if there has been a break in service of	
		0-23 months	- 24 months or more
Confidential	0 to 14 yrs. 11 mos 15 yrs. or more	None (note 1) NACLC.	NACLC
Secret; "L"	0 to 9 yrs 11 mos 10 yrs. or more	None (note 1). NACLC	
Top Secret, SCI; "Q"	0 to 4 yrs. 11 mos 5 yrs or more	None (note 1) SSBI-PR.	SSBI

Note: As a minimum, review an updated Standard Form 84 and applicable records. A reinvestigation (NACLC or SSBI-PR) is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968.

Subpart C—Guidelines for Temporary Access

§ 147.28 Introduction.

The following minimum investigative standards, implementing section 3.3 of Executive Order 12968, *Access to Classified Information*, are established for all United States Government and military personnel, consultants, contractors, subcontractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information before the appropriate investigation can be completed and a final determination made.

§ 147.29 Temporary eligibility for access.

Based on a justified need meeting the requirements of section 3.3 of Executive Order 12968, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated, where official functions must be performed prior to completion of the investigation and

adjudication process. The temporary eligibility will be valid until completion of the investigation and adjudication; however, the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation.

§ 147.30 Temporary eligibility for access at the confidential and secret levels and temporary eligibility for "L" access authorization.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and submission of a request for an expedited National Agency Check with Local Agency Checks and Credit (NACLC).

§ 147.31 Temporary eligibility for access at the top secret levels and temporary eligibility for "Q" access authorization: For someone who is the subject of a favorable investigation not meeting the investigative standards for access at those levels.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and expedited submission of a request for a Single Scope Background Investigation (SSBI).

§ 147.32 Temporary eligibility for access at the top secret and SCI levels and temporary eligibility for "Q" access authorization: For someone who is not the subject of a current, favorable personnel or personnel-security investigation of any kind.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, immediate submission of a request for

immediate submission of a request for an expedited Single Scope Background Investigation (SSBI), and completion and favorable review by the appropriate adjudicating authority of relevant criminal history and investigative records of the Federal Bureau of Investigation and of information in the Security/Suitability Investigations Index (SII) and the Defense Clearance and Investigations Index (DCII).

§ 147.33 Additional requirements by agencies.

Temporary eligibility for access must satisfy these minimum investigative standards, but agency heads may establish additional requirements based on the sensitivity of the particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access. However, no additional requirements shall exceed the common standards for background investigations developed under section 3.2(b) of Executive Order 12968. Temporary eligibility for access is valid only at the agency granting it and at other agencies who expressly agree to accept it and acknowledge understanding of its investigative basis. It is further subject to limitations specified in sections 2.4(d) and 3.3 of Executive Order 12968, *Access to Classified Information*.

Dated: January 22, 1998.

L.M. Bynum.

Alternate OSD Federal Register Liaison
Officer, Department of Defense.
(FR Doc. 98-1955 Filed 1-29-98; 8:45 am)
BILLING CODE 5000-04-M

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 148

RIN 0790-AG55

National Policy on Reciprocity of Facilities and Guidelines for Implementation of Reciprocity

AGENCY: Department of Defense.

ACTION: Interim final rule.

SUMMARY: This rule is published to make physical facilities available for reciprocal use in the storage of classified information. Once a facility has been certified as suitable for classified use by one organization, it may also be used by another for like purposes. No impact on the public is foreseen.

DATES: This rule is effective September 16, 1997. Comments must be received by March 31, 1998.

ADDRESSES: Forward comments to the Security Policy Board Staff, 1215 Jefferson Davis Highway, Suite 1101, Arlington, VA 22202.

FOR FURTHER INFORMATION CONTACT: Mr. T. Thompson, 703-602-9969.

SUPPLEMENTARY INFORMATION:

Executive Order 12866, Regulatory Planning and Review

It has been determined that this interim rule (32 CFR part 148) is not a significant regulatory action. The rule does not:

(1) Have an annual effect to the economy of \$100 million or more or adversely affect in a material way the economy; a section of the economy; productivity; competition; jobs the environment; public health or safety; or State, local, or tribal governments or communities;

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency;

(3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive Order.

Public Law 96-354, Regulatory Flexibility Act (5 U.S.C. 601)

It has been certified that this rule is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities. This part will streamline personnel security clearance procedures and make the process more efficient.

Public Law 96-511, Paperwork Reduction Act (44 U.S.C. Chapter 35)

It has been certified that this part does not impose any reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995.

List of Subjects in 32 CFR Part 148

Classified information, Investigations, Security measures.

Accordingly, Title 32 of the Code of Federal Regulations, Chapter I, subchapter C is amended to add part 148 to read as follows:

PART 148—NATIONAL POLICY AND IMPLEMENTATION OF RECIPROCITY OF FACILITIES

Subpart A—National Policy on Reciprocity of Use and Inspections of Facilities

- 148.1 Interagency reciprocal acceptance.
- 148.2 Classified programs.
- 148.3 Security review.
- 148.4 Policy documentation.
- 148.5 Identification of the security policy board.
- 148.6 Agency review.

Subpart B—Guidelines for the Implementation and Oversight of the Policy on Reciprocity of Use and Inspections of Facilities

- 148.10 General.
- 148.11 Policy.
- 148.12 Definitions.
- 148.13 Responsibilities.
- 148.14 Procedures.

Authority: E.O. 12968 (60 FR 40245, 3 CFR 1995 Comp., p. 391.)

Subpart A—National Policy on Reciprocity of Use and Inspections of Facilities

§ 148.1 Interagency reciprocal acceptance.

Interagency reciprocal acceptance of security policies and procedures for approving, accrediting, and maintaining the secure posture of shared facilities will reduce aggregate costs, promote interoperability of agency security systems, preserve vitality of the U.S. industrial base, and advance national security objectives.

§ 148.2 Classified programs.

Once a facility is authorized, approved, certified, or accredited, all U.S. Government organizations desiring to conduct classified programs at the facility at the same security level shall accept the authorization, approval, certification, or accreditation without change, enhancements, or upgrades. Executive Order, Safeguarding Directives, National Industrial Security Program Operating Manual (NISPOM), the NISPOM Supplement, the Director of Central Intelligence Directives, interagency agreements, successor documents, or other mutually agreed upon methods shall be the basis for such acceptance.

§ 148.3 Security review.

After initial security authorization, approval, certification, or accreditation, subsequent security reviews shall normally be conducted no more frequently than annually.

Additionally, such reviews shall be aperiodic or random, and be based upon risk management principles. Security reviews may be conducted "for cause", to follow up on previous findings, or to

accomplish close-out actions. Visits may be made to a facility to conduct security support actions, administrative inquiries, program reviews, and approvals as deemed appropriate by the cognizant security authority or agency.

§ 148.4 Policy documentation.

Agency heads shall ensure that any policy documents their agency issues setting out facilities security policies and procedures incorporate the policy set out herein, and that such policies are reasonable, effective, efficient, and enable and promote interagency reciprocity.

§ 148.5 Identification of the security policy board.

Agencies which authorize, approve, certify, or accredit facilities shall provide to the Security Policy Board Staff a points of contact list to include names and telephone numbers of personnel to be contacted for verification of authorized, approved, certified, or accredited facility status. The Security Policy Board Staff will publish a comprehensive directory of points of contact.

§ 148.6 Agency review.

Agencies will continue to review and assess the potential value added to the process of co-use of facilities by development of electronic data retrieval across government. As this review continues, agencies creating or modifying facilities databases will do so in a manner which facilitates community data sharing, interest of national defense or foreign policy.

Subpart B—Guidelines for the Implementation and Oversight of the Policy on Reciprocity of use and Inspections of Facilities

§ 148.10 General.

(a) Redundant, overlapping, and duplicative policies and practices that govern the co-use of facilities for classified purposes have resulted in excessive protection and unnecessary expenditure of funds. Lack of reciprocity has also impeded achievement of national security objectives and adversely affected economic and technological interest.

(b) Interagency reciprocal acceptance of security policies and procedures for approving, accrediting, and maintaining the secure posture of shared facilities will reduce the aggregate costs, promote interoperability of agency security systems, preserve the vitality of the U.S. industrial base, and advance national security objectives.

(c) Agency heads, or their designee, are encouraged to periodically issue

written affirmations in support of the policies and procedures prescribed herein and in the Security Policy Board (SPB) policy, entitled "Reciprocity of Use and Inspections of Facilities."

(d) The policies and procedures prescribed herein shall be applicable to all agencies. This document does not supersede the authority of the Secretary of Defense under Executive Order 12829 (58 FR 3479, 3 CFR 1993 Comp., p. 570); the Secretary of Energy or the Chairman of the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of State under the Omnibus Diplomatic Security and Anti-Terrorism Act of 1986; the Secretaries of the military departments and military department installation Commanders under the Internal Security Act of 1950; the Director of Central Intelligence under the National Security Act of 1947, as amended, or Executive Order 12333; the Director of the Information Security Oversight Office under Executive Order 12829 or Executive Order 12958 (60 FR 19825, 3 CFR 1995 Comp., p. 333); or substantially similar authority instruments assigned to any other agency head.

§ 148.11 Policy.

(a) Agency heads, or their designee, shall ensure that security policies and procedures for which they are responsible are reasonable, effective, and efficient, and that those policies and procedures enable and promote interagency reciprocity.

(b) To the extent reasonable and practical, and consistent with US law, Presidential decree, and bilateral and international obligations of the United States, the security requirements, restrictions, and safeguards applicable to industry shall be equivalent to those applicable within the Executive Branch of government.

(c) Once a facility is authorized approved, certified, or accredited, all government organizations desiring to conduct classified programs at the facility at the same security level shall accept the authorization, approval, certification, or accreditation without change, enhancements, or upgrades.

§ 148.12 Definitions.

Agency. Any "executive agency," as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the Executive Branch that comes into possession of classified information.

Classified Information. All information that requires protection under Executive Order 12958, or any of

its antecedent orders, and the Atomic Energy Act of 1954, as amended.

Cognizant Security Agency (CSA).

Those agencies that have been authorized by Executive Order 12829 to establish an industrial security program for the purpose of safeguarding classified information disclosed or released to industry.

Cognizant Security Office (CSO). The office or offices delegated by the head of a CSA to administer industrial security in a contractor's facility on behalf of the CSA.

Facility. An activity of a government agency or cleared contractor authorized by appropriate authority to conduct classified operations or to perform classified work.

Industry. Contractors, licensees, grantees, and certificate holders obligated by contract or other written agreement to protect classified information under the National Industrial Security Program.

National Security. The national defense and foreign relations of the United States.

Senior Agency Official. Those officials, pursuant to Executive Order 12958, designated by the agency head who are assigned the responsibility to direct and administer the agency's information security program.

§ 148.13 Responsibilities.

(a) Each Senior Agency Official shall ensure that adequate reciprocity provisions are incorporated within his or her regulatory issuances that prescribe agency safeguards for protecting classified information.

(b) Each Senior Agency Official shall develop, implement, and oversee a program that ensures agency personnel adhere to the policies and procedures prescribed herein and the reciprocity provisions of the National Industrial Security Program Operating Manual (NISPOM).

(c) Each Senior Agency Official must ensure that implementation encourages reporting of instances of non-compliance, without fear of reprisal, and each reported instance is aggressively acted upon.

(d) The Director, Information Security Oversight Office (ISOO), consistent with his assigned responsibilities under Executive Order 12829, serves as the central point of contact within Government to consider and take action on complaints and suggestions from industry concerning alleged violations of the reciprocity provisions of the NISPOM.

(e) The Director, Security Policy Board Staff (D/SPBS) or his/her designee, shall serve as the central point

of contact within Government to receive from Federal Government employees alleged violations of the reciprocity provisions prescribed herein and the policy "Reciprocity of Use and Inspections of Facilities" of the SPB.

§ 148.14 Procedures.

(a) Agencies that authorize, approve, certify, or accredit facilities shall provide to the SPB Staff a points of contact list to include names and telephone numbers of personnel to be contacted for verification of the status of facilities. The SPB Staff will publish a comprehensive directory of agency points of contact.

(b) After initial security authorization, approval, certification, or accreditation, subsequent reviews shall normally be conducted no more frequently than annually. Additionally, such reviews shall be aperiodic or random, and be based upon risk-management principles. Security Reviews may be conducted "for cause", to follow up on previous findings, or to accomplish close-out actions.

(c) The procedures employed to maximize interagency reciprocity shall be based primarily upon existing organizational reporting channels. These channels should be used to address alleged departures from established reciprocity requirements and should resolve all, including the most egregious instances of non-compliance.

(d) Two complementary mechanisms are hereby established to augment existing organizational channels: (1) An accessible and responsive venue for reporting and resolving complaints/reported instances of non-compliance. Government and industry reporting channels shall be as follows:

(1) *Government.* (A) Agency employees are encouraged to bring suspected departures from applicable reciprocity requirements to the attention of the appropriate security authority in accordance with established agency procedures.

(B) Should the matter remain unresolved, the complainant (employee, Security Officer, Special Security Officer, or similar official) is encouraged to report the matter formally to the Senior Agency Official for resolution.

(C) Should the Senior Agency Official response be determined inadequate by the complainant, the matter should be reported formally to the Director, Security Policy Board Staff (D/SPBS). The D/SPBS, may revisit the matter with the Senior Agency Official or refer the matter to the Security Policy Forum as deemed appropriate.

(D) Should the matter remain unresolved, the Security Policy Forum may consider referral to the SPB, the agency head, or the National Security Council as deemed appropriate.

(ii) *Industry.* (A) Contractor employees are encouraged to bring suspected departures from the reciprocity provisions of the NISPOM to the attention to their Facility Security Officer (FSO) or Contractor Special Security Officer (CSSO), as appropriate, for resolution.

(B) Should the matter remain unresolved, the complainant (employee, FSO, or CSSO) is encouraged to report the matter formally to the Cognizant Security Office (CSO) for resolution.

(C) Should the CSO responses be determined inadequate by the complainant, the matter should be reported formally to the Senior Agency Official within the Cognizant Security Agency (CSA) for resolution.

(D) Should the Senior Agency Official response be determined inadequately by the complainant, the matter should be reported formally to the Director, Information Security Oversight Office (ISOO) for resolution.

(E) The Director, ISOO, may revisit the matter with the Senior Agency Official or refer the matter to the agency head or the National Security Council as deemed appropriate.

(2) An annual survey administered to a representative sampling of agency and private sector facilities to assess overall effectiveness of agency adherence to applicable reciprocity requirements.

(i) In coordination with the D/SPBS, the Director, ISOO, as Chairman of the NISP Policy Advisory Committee (NISPPAC), shall develop and administer an annual survey to a representative number of cleared contractor activities/employees to assess the effectiveness of interagency reciprocity implementation. Administration of the survey shall be coordinated fully with each affected Senior Agency Official.

(ii) In coordination with the NISPPAC, the D/SPBS shall develop and administer an annual survey to a representative number of agency activities/personnel to assess the effectiveness of interagency reciprocity implementation. Administration of the survey shall be coordinated fully with each affected Senior Agency Official.

(iii) The goal of annual surveys should not be punitive but educational. All agencies and departments have participated in the crafting of these facilities policies, therefore, non-compliance is a matter of internal education and direction.

(e) Agencies will continue to review and assess the potential value added to the process of co-use of facilities by development of electronic data retrieval across government.

Dated: January 22, 1998.

L.M. Bynum,
Alternate OSD Federal Register Liaison
Officer, Department of Defense.
[FR Doc. 98-1956 Filed 1-29-98; 8:45 am]
BILLING CODE 5000-04-M

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 149

RIN 0790-AG58

National Policy on Technical Surveillance Countermeasures

AGENCY: Department of Defense.

ACTION: Interim final rule.

SUMMARY: This rule is published to limit the use of technical surveillance countermeasures within the boundaries of the U.S. to cases where there is a reasonable showing of threat. No impact on the public is foreseen.

DATES: This rule is effective September 16, 1997. Comments must be received by March 31, 1998.

ADDRESSES: Forward comments to the Security Policy Board Staff, 1215 Jefferson Davis Highway, Suite 1101, Arlington, VA 22202.

FOR FURTHER INFORMATION CONTACT: Mr. T. Thompson, 703-602-9969.

SUPPLEMENTARY INFORMATION:

Executive Order 12866, Regulatory Planning and Review

It has been determined that this interim rule (32 CFR Part 149) is not a significant regulatory action. The rule does not:

"(1) Have an annual effect to the economy of \$100 million or more or adversely affect in a material way the economy; a section of the economy; productivity; competition; jobs; the environment, public health or safety; or State, local, or tribal governments or communities;

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by other Agency;

(3) Materially alter the budgetary impact of entitlements, grants, user fee or loan programs, or the rights and obligations of recipients thereof; or

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive Order.

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* 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
001a. memo	For James Hall from Glyn Davies. Subject: Anthony Lake Security 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 [1]

2006-1066-F
vz870

RESTRICTION CODES

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

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

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]

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]

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.

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.

[001a]

P6/(b)(6)

Withdrawal/Redaction Marker

Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001b. draft	For James Hall from Glyn Davies. Subject: Anthony Lake Security 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 [1]

2006-1066-F
vz870

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.

[001b]

P6/(b)(6)

~~Glyn T. Davies
Executive Secretary~~

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 S.I.C.:**→ Security**TX.*

ACTION: DAVIES SGD MEMO

DUE DATE: 22 APR 97 STATUS: C

STAFF OFFICER: BAKER

LOGREF:

FILES: NS

NSCP:

CODES:

DOCUMENT DISTRIBUTION

FOR ACTIONFOR CONCURRENCEFOR INFO~~BAKER~~
KRECKO
LEARY
NSC CHRONCOMMENTS: _____

DISPATCHED BY _____ DATE _____ BY HAND W/ATTCH

OPENED BY: NSTMH

CLOSED BY: NSMEC

DOC 2 OF 2

UNCLASSIFIED

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

UNCLASSIFIED

Withdrawal/Redaction Marker

Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
002. memo	For Samuel Berger from James Baker and Mary McCarthy. Subject: Defense Adjudication. (5 pages)	07/08/1998	P6/b(6)

COLLECTION:

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

FOLDER TITLE:

Personnel Security [1]

2006-1066-F

vz870

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]

BENJAMIN A. GILMAN, New York
Chairman

LEE H. MAMILLON, Indiana
Ranking Democratic Member

WILLIAM F. GOODLING, Pennsylvania
JAMES A. LEACH, Iowa
HENRY J. HYDE, Illinois
DOUG BERTUTER, Massachusetts
CHRISTOPHER H. SMITH, New Jersey
DAN BURTON, Indiana
ELTON GALLEGLY, California
JESSE ROSENTHAL, Florida
GARY BALLINGER, North Carolina
DANA ROHRBAUGH, California
DONALD A. MANZULLO, Illinois
EDWARD R. ROYCE, California
PETER T. KING, New York
JAY KING, California
STEVEN J. CABOT, Ohio
MARSHALL "MARK" SANFORD, South Carolina
MATT SALMON, Arizona
AMO HOUGHTON, New York
TOM CAMPBELL, California
JON FOX, Pennsylvania
JOHN M. McHUGH, New York
LINDSEY O. GRAHAM, South Carolina
ROY BLUNT, Missouri
JERRY MORAN, Kansas

ONE HUNDRED FIFTH CONGRESS
CONGRESS OF THE UNITED STATES
COMMITTEE ON INTERNATIONAL RELATIONS
HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515

TELEPHONE: (202) 225-5021

February 5, 1998

BAM DEJONSON, Connecticut
TON LANTOS, California
HOWARD L. BERMAN, California
GARY L. ACKERMAN, New York
ENI F. N. FALEOMAEVEGA, American Samoa
MATTHEW G. MARTINEZ, California
DONALD M. PAYNE, New Jersey
ROBERT E. ANDREWS, New Jersey
ROBERT MENENDEZ, New Jersey
SPERRO BROWN, Ohio
CYNTHIA A. MCINNEY, Georgia
ALCEE L. HASTINGS, Florida
PAT DANNER, Missouri
EARL F. HILLARD, Alabama
BRAD SHERMAN, California
ROBERT VICKLER, Florida
STEVEN R. ROTHMAN, New Jersey
BOB CLEMENT, Tennessee
BILL LUTHER, Minnesota
JIM DAVIS, Florida

MICHAEL H. VAN CUSEN
Democratic Chief of Staff

RICHARD J. GARRON
Chief of Staff

William S. Cohen
Secretary of Defense
Department of Defense
The Pentagon
Washington, D.C. 20301-1155

Dear Secretary Cohen:

We write to seek a positive decision on the application for a Top Secret security clearance for Amos Hochstein, consistent with U.S. law and policy. We believe that granting clearance in this case would comply with our mutual concern for safeguarding United States security interests.

Amos Hochstein, Democratic staff director for the International Relations Subcommittee on International Economic Policy and Trade, was nominated for clearance in December 1996. We understand that Mr. Hochstein has cooperated fully with your Office of Personnel and Security in resolving questions raised by his U.S.-Israeli dual citizenship. But, we also understand from that office's October 2, 1997 letter, that Mr. Hochstein's use of his Israeli passport to enter and exit Israel, as required by Israeli law, is considered problematic for granting of the clearance.

We believe that Amos Hochstein has provided clear evidence of his allegiance to the United States, including signing a statement that (1) he would seriously consider renouncing his Israeli citizenship if asked to do so; (2) he has no future military obligation in Israel and does not intend to volunteer; and (3) he does not exercise the privileges of citizenship such as voting in the Israeli elections. Moreover since his employment by the Committee on December 1, 1996, Mr. Hochstein has shown himself to be a loyal employee, who has not shown preference toward Israel in matters before the Committee.

Mr. Hochstein's use of his Israeli passport to travel to Israel is required by Israeli law and appears to be sanctioned by U.S. law and policy. Complying with the legal obligations of Israeli citizenship, under sanction of U.S. law, should not mitigate against the granting of a security clearance. Department of Defense regulation 5200.2-R states that use of a foreign passport is a "condition that could raise a security concern [because it would] indicate a preference for a foreign country over the United States." Israel, however, requires its citizens to use their Israeli

William S. Cohen
February 5, 1998
Page Two

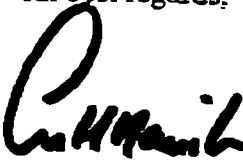
passports to enter and exit Israel. The U.S. Government recognizes this requirement in its dual citizenship arrangements with Israel, as demonstrated by the State Department's Consular Information Sheet which advises U.S. citizens on travel to Israel (enclosed). Because the use by any dual citizen of his Israeli passport is required by the Israeli Government and that obligation is recognized by the U.S. Government, Mr. Hochstein's compliance should not be judged to be a "preference for the foreign country over the United States."

Requiring Mr. Hochstein to relinquish the Israeli passport would raise fundamental issues that go to the core of the U.S.-Israeli relationship and brings into question the status of the significant group of U.S. citizens who are recognized by the U.S. Government to be able to hold a dual U.S.-Israeli citizenship. Since the use of the passport is one of many factors that you may use to determine whether to grant a security clearance -- and in no case is it an absolute bar -- we hope you will not assign it undue significance, in light of these facts and the positive factors in the regulation 5200.2-R that Mr. Hochstein meets.

We share your goal of providing the utmost reasonable protection to United States' security interests. If your concerns would be assuaged by having more direct control over Mr. Hochstein's access to his Israeli passport, we would suggest that one alternative for granting clearance is for you to designate a security office at the Committee or within the Executive Branch that would hold Mr. Hochstein's Israeli passport, to ensure that it is not being used except in the narrow circumstances we have described. Mr. Hochstein would get the passport from such office only for travel to Israel, and not for any other other reasons. We would view such an option as a solution that both safeguards security concerns and offers a reasonable approach that upholds U.S. policy on U.S.-Israeli citizenship.

We hope that you will positively assess the case, with the mitigating factors in mind, or will discuss a compromise solution for clearance, if necessary. We appreciate your attention to this matter of mutual concern.

With best regards,


Lee H. Hamilton

Sincerely,


Sam Gejdenson

cc: Samuel R. Berger
National Security Advisor

Enclosure

FROM : CA/OCS

202 547 3732

1997.12-09

16:59

8118 P.04/87

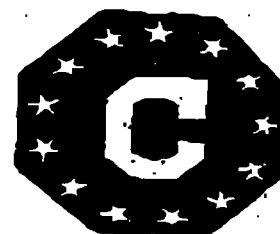


U. S. Department of State
Bureau of Consular Affairs
Washington, DC 20520

For recorded travel information, call 202-647-5225

Internet Address: travel.state.gov

For information by fax, call 202-647-3000 from your fax machine



Consular Information Sheet

Israel & The Occupied Territories

(Including Areas Subject To The Jurisdiction Of
The Palestinian Interim Self-Government Authority)

January 22, 1997

Country Description: The state of Israel is a parliamentary democracy with a modern economy. Tourist facilities are widely available. Israel occupied the West Bank, Gaza Strip, Golan Heights, and East Jerusalem as a result of the 1967 war. Pursuant to negotiations between Israel and the Palestinians, an elected Palestinian Authority now exercises jurisdiction in most of Gaza and most of the major cities of the West Bank. Palestinian Authority police have responsibilities for keeping order in those areas and the Palestinian Authority exercises a range of civil functions in other areas of the West Bank. The West Bank city of Hebron is still under the control of the Israeli Army. Areas of Israeli and Palestinian Authority responsibilities and jurisdiction in the West Bank and Gaza are complex. Definitive information on entry, customs requirements, arrests and other matters in the West Bank and Gaza may not be available and is subject to change without prior notice.

Embassy/Consulate Location and Sources of Assistance: The U.S. Embassy in Tel Aviv, Israel, is located at 71 Hayarkon Street. The U.S. mailing address is PSC 98, Box 100, APO AE 09830. The telephone number is (972) (3) 519-7575. The after hours number is 519-7551. The fax number is 972-3-516-0315. The e-mail address is acs.ameet-telaviv@dos.us-state.gov. The Consular Section of the U.S. Embassy in Tel Aviv should be contacted for information and help in the following areas: Israel, the Gaza Strip, and ports of entry at Ben Gurion Airport and the northern (Jordan River) and Southern (Arava) border crossings connecting Israel and Jordan.

The Consular Section of the U.S. Consulate General in Jerusalem is located at 27 Nablus Road. The U.S. mailing address is PSC 98, Box 100, APO AE 09830. The telephone number is (972) (2) 625-3288. The after hours number is 625-3201/2. The fax number is (972) (2) 627-2233. The U.S. Consulate should be contacted for information and help in the following areas: West and East Jerusalem, the West Bank, and border crossings at the Allenby Bridge, connecting Jordan with the West Bank.

There is a U.S. Consular Agent in Haifa, at 13 Jerusalem Street, Haifa 33132, telephone (972) (4) 867-0616.

Entry Requirements:

Israel: Passports, an onward or return ticket, and proof of sufficient funds are required for entry. A three-month visa may be issued for no charge upon arrival, and may be renewed. Anyone who has been refused entry or experienced difficulties with his/her visa status during a previous visit, or who has overstayed a visa, can obtain information from the Israeli Embassy or nearest consulate regarding the advisability of attempting to return to Israel. Permission must be obtained from Israel for anyone attempting to claim the status of a returning resident.

Palestinian Authority: Except during periods of closures, U.S. citizens may enter and exit Gaza and the West Bank on a U.S. passport with an Israeli visa. It is not necessary to obtain a visitor's permit from the Palestinian Authority. Private vehicles frequently encounter long delays entering or leaving Gaza and may also expect to be stopped at checkpoints entering or leaving the West Bank. Palestinian Americans with residency permits for the West Bank and Gaza are subject to the same travel restrictions as other Palestinians residing in those areas.

FROM : CR/DES

202 647 3752

1997.12-09

17:00

5116 P.05/87

Israel-Jordan Crossings: International crossing points are now in operation between Israel and Jordan at Arava (Wadi Al-Arabah) crossing in the south and the Jordan River crossing (Sheikh Hussein Bridge) in the north. Prior visas are not necessary for American citizens using these two crossing points, but travelers will have to pay a fee. Visas should be obtained in advance for those wanting to cross the Allenby Bridge which links Jordan and the occupied West Bank. (Note: Palestinian Americans with residency in the West Bank must cross into Jordan using the Allenby Bridge.) Procedures for all crossings into Jordan are subject to frequent changes.

For further entry information, travelers may contact the Israeli Embassy at 3514 International Dr., N.W., Washington, D.C. 20008, telephone (202) 364-5500, or the nearest Israeli consulate general in Los Angeles, San Francisco, Miami, Atlanta, Chicago, New Orleans, Boston, New York, Philadelphia, or Houston.

Customs Requirements: Video cameras, among other items, must be declared upon entry to Israel and travelers carrying these items must go through the red zone at customs. Definitive information on customs requirements for the Palestinian Authority is not available.

Security Measures: Israel has strict security measures that may affect visitors. Prolonged questioning and detailed searches may take place at the time of entry and/or departure at all points of entry to Israel, including entry from any of the areas under Palestinian jurisdiction. American citizens with Arab surnames may expect close scrutiny at Ben Gurion Airport and the Allenby Bridge from Jordan. For security reasons, delays or obstacles in bringing in or departing with cameras or electronics equipment are not unusual. During searches and questioning, access may be denied to U.S. consular officers, lawyers, or family members. Definitive information on security measures in the Palestinian Authority is not available.

Areas of Instability:

West Bank and Gaza: During periods of unrest, the West Bank and Gaza are sometimes closed off by the Israeli Government. Travel restrictions may be imposed with little or no warning. Following the series of suicide bombings in Israel in February and March 1996, strict security measures were put into effect. Movement of Palestinians (including Palestinian Americans) and foreign passport holders has been severely impaired.

Demonstrations by Palestinians and Israelis in the West Bank have led to confrontations and clashes with the police, with some turning deadly. Stone throwing and other forms of protest can occur without warning and escalate quickly.

In view of the continued potential for violence and unrest in the West Bank and Gaza, the State Department advises all American citizens to avoid travel to these areas, except for daylight visits to Bethlehem, Jericho, Highway 1 from Jerusalem to the Dead Sea, Route 90 through the Jordan Valley, and tourist sites along these routes. This includes the Inn of the Samaritan, Nebi Musa, St. George's Monastery, Mount of Temptation Monastery, Qumran, and Quallah Water Park. The consular section of the Consulate General, located at 27 Nablus Road in East Jerusalem, is safe and accessible to all visitors.

The U.S. government instituted and continues to maintain tight security procedures regarding travel of U.S. government employees, officials, and dependents to the Gaza Strip and the West Bank. Frequently, U.S. government employees are instructed not to travel at all to these areas. Travel guidelines for U.S. government employees may change at any time.

The Palestinian police force has been established in Gaza and the major cities of the West Bank which are under Palestinian jurisdiction. Joint Israeli/Palestinian police patrols and checkpoints may be encountered. Guns are often owned by Israeli civilians and by Palestinians in Gaza.

General Precautions: Travel on strike days or after dark is not recommended. Tourists using public transportation or traveling by car in areas less frequented by tourists are at risk. Vehicles have been damaged, with rental cars in particular being targeted.

Jerusalem: In Jerusalem, travelers can reduce their risk of being involved in violent incidents by traveling in groups, avoiding the old city at night, except for the Jewish Quarter, and

FROM : CR/OCS

202 647 3732

1997-12-89

17:01

8:18 P. 87

exercising caution at religious sites on holy days, Fridays, and Saturdays. Most roads into Ultra-orthodox Jewish neighborhoods are blocked off on Saturdays. Assaults on secular visitors, either for being in cars or for being "immodestly dressed," have been known to occur in these neighborhoods.

In the North: In the Golan Heights, there are live land mines in many areas, and some minefields have not been clearly marked or fenced. Visitors who walk only on established roads or trails will reduce the risk of injury from mines. Rocket attacks from Lebanese territory can occur without warning close to the northern border of Israel.

Driving and Road Conditions: There is a high rate of fatalities relating to auto accidents, and caution should be exercised. While the roads in Israel are well built, the roads in Gaza and most of the West Bank are of poor quality.

Terrorism: Although U.S. citizens have not been specifically targeted for attack, several terrorist incidents in the West Bank and Gaza, as well as within Israel, have killed or injured U.S. citizens. Several violent attacks have involved passengers on buses and at bus stops. The U.S. Embassy and the Consulate General have warned their employees and American citizens to avoid travel on public buses, as well as congregating at bus stops and other crowded areas. This restriction does not apply to tour buses.

Arrests in the West Bank and Gaza Strip: U.S. citizens arrested or detained in the West Bank on suspicion of security offenses often are not permitted to communicate with consular officials, lawyers, or family members in a timely manner during the interrogation period of their case. Youths over the age of fourteen have been detained and tried as adults. The U.S. Embassy is not normally notified of the arrests of Americans in the West Bank by Israeli authorities, and access to detainees is frequently delayed. Notification may be more rapid if the arrested American shows a U.S. passport to Israeli officials as proof of U.S. citizenship.

Israeli authorities should notify the U.S. Embassy when an American is arrested by Palestinian police in the West Bank or Gaza, and requests by the U.S. consul to visit arrested Americans should be communicated to the Palestinian Authority through a joint Israeli-Palestinian committee. Significant delays in notification and consular access may occur under these procedures.

Medical Facilities: Modern medical care and medicines are available in Israel. However, some hospitals in Israel and most hospitals in the Gaza Strip and the West Bank fall below U.S. standards. Travelers can find information written in English about emergency medical facilities and after-hours pharmacies in the "Jerusalem Post" newspaper. Doctors and hospitals often expect immediate cash payment for health services. U.S. medical insurance is not always valid outside the United States. Supplemental medical insurance with specific overseas coverage has proven useful. The international traveler's hotline at the Centers for Disease Control and Prevention at telephone (404) 332-4559 has additional health information. The Internet site is <http://cdc.gov>. Travelers from regions where contagious diseases are prevalent may need to show shot records before entry.

Information on Crime: The crime rate is moderate in Israel, the Gaza Strip, and the West Bank. The loss or theft of a U.S. passport should be reported immediately to local police and the nearest U.S. embassy or consulate. Useful information on safeguarding valuables, protecting personal security, and other matters is provided in the Department of State pamphlets, "A Safe Trip Abroad" and "Tips for Travelers to the Middle East and North Africa," available from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

Drug Penalties: U.S. citizens are subject to the laws of the territory in which they are traveling. Penalties for possession, use, or trafficking in illegal drugs are severe in Israel, and convicted offenders can expect jail sentences and fines. The Palestinian Authority also has strict penalties for drug use by persons under its jurisdiction.

Court Jurisdiction: Under Israel's judicial system, the Rabbinical courts exercise jurisdiction over all Jewish citizens and residents of Israel in cases of marriage and divorce and related

FROM : CR/CCS

202 547 5752

1997.12-09

17:02

0110 P.07/07

Issues such as support and child custody. Rabbinical courts can also impose sanctions, including jail terms and restrictions against leaving the country, on individuals married in a Jewish religious ceremony who, in case of divorce, refuse to give their spouses a religious divorce ("GET"). In some cases, Jewish Americans, who entered Israel as tourists, have become defendants in divorce cases filed against them in a Rabbinical court in Israel by their American spouses who are seeking a religious divorce that the defendants have refused to give. These Americans have been detained in Israel for prolonged periods while the Israeli courts consider whether such individuals have sufficient ties to Israel to establish Rabbinical court jurisdiction. The Rabbinical courts have also detained in the country a Jewish American tourist who has been sued for support by his spouse in the United States. Jewish American visitors should be aware that they may be subject to involuntary and prolonged stays in Israel if a case is filed against them in a Rabbinical Court. This may occur even when the marriage took place in the U.S. and/or the spouse seeking relief is not present in Israel.

Dual Nationality: Israeli citizens naturalized in the United States retain their Israeli citizenship, and their children are considered Israeli citizens as well. In addition, children born in the United States to Israeli parents acquire both U.S. and Israeli nationality at birth. Israeli citizens, including dual nationals, are subject to Israeli laws requiring service in Israel's armed forces. U.S.-Israeli dual nationals of military age who do not wish to serve in the Israeli armed forces may contact the Israeli Embassy to obtain proof of exemption or deferment from Israeli military service before going to Israel. Otherwise, they may not be able to leave the country without doing military service. Israeli citizens, including dual nationals, must enter and depart Israel on their Israeli passports. (Note: U.S.-Israeli dual citizens must enter and depart the U.S. on their U.S. Passports.)

Palestinian-American citizens with residency rights in Israel, Gaza, or the West Bank are subject to the same regulations as other resident Palestinians. This may require them to depart these areas with Palestinian travel documents or (for residents of Jerusalem) laissez-passers with re-entry permits approved by the Israeli Ministry of Interior.

Registration: The State Department advises American citizens who plan to be in the region for a substantial period of time to register at the U.S. Embassy in Tel Aviv or the U.S. Consulate General in Jerusalem. When registering, U.S. citizens can obtain updated information on travel and security in the area.

No. 97-007

This replaces the Consular Information Sheet dated August 7, 1996, to provide new information about the role of Rabbinical courts in Israel and their potential implications for Jewish American tourists.

more in full credit

Wash. Hqs. Issues sent or. Army. / sent.

Am. rights fully.

Adverse impact in past better to w/dow

risk. Israeli noted. Fairly like him. Israeli passport.
2 in a year. 1995.

1) passport (symbolic)

2) Travel

3) full disc

Turn in passport would mitigate.

Gen. Am. to not have to travel.

Sufficiently separate not to exercise a foreign presence in dealing with
classified.

Indirect. While person.

⇒ Risk management.

⇒ Dual national

⇒ Use other places.

Withdrawal/Redaction Marker

Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
003. email	From Karl Hoffman to Various. Subject: Short Notice Vetting. (2 pages)	06/10/1998	P1/b(1)

COLLECTION:

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

FOLDER TITLE:

Personnel Security [1]

2006-1066-F
vz870

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

January 5, 1998

ACTION

MEMORANDUM FOR DONALD L. KERRICK

FROM: JAMES BAKER ^{JB}

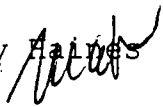
SUBJECT: Access to NSC Background Investigations & Process
for NSC Suitability Determinations

The White House Security Office has requested a revised list of persons authorized access to FBI background materials on NSC personnel. The attached memorandum from Glyn Davies provides such an update.

The memorandum also memorializes the process by which the NSC, in consultation with the Office of White House Counsel, will make suitability determinations. In reaching this formulation we considered carefully whether such decisions should ultimately be made by the White House Counsel or the NSC. Counsel's Office argued that if they were to serve as ultimate arbiter of suitability, WHC rather than NSC, should make all the NSC's suitability determinations and not just those in the difficult cases we raise. As a result, we recommend the formula above: NSC in consultation with WHC. This will allow the NSC to control the tempo of its own security and suitability decisions and is, I believe, consistent with the Front Office's own view that the APNSA ultimately should decide who works on the NSC staff.

The NSC Security Officer will continue to adjudicate, or verify, access to national security information for NSC staff using the standards contained in E.O. 12968 and corresponding adjudicative guidelines. The Secret Service will continue to evaluate employees from the perspective of potential threats to the President. The Office of White House Security will continue to serve as gatekeeper for BI requests and ensure the necessary steps have been taken before issuance of a permanent pass. However, as the attached memorandum underscores, where the NSC has favorably adjudicated security and suitability, a permanent pass will be issued unless there is a separate basis for denying access, such as a failed tax check or drug test.

Concurrence by:

Mary  and Jim  Hall

RECOMMENDATION

That you and Glyn sign the attached signature page and that you authorize Glyn Davies to sign the memorandums at Tabs I and II.

Approve _____ Disapprove _____

Attachments

Tab I Memorandum for Chuck Easley Re Authorization
for Review or Process BI Files for NSC
Tab A Prior NSC Authorization for BI Access
Tab II Memorandum for Chuck Easley Re Approval and
Initiation of BI Access for NSC

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

MEMORANDUM FOR CHARLES C. EASLEY

FROM: GLYN DAVIES

SUBJECT: Updated Authorization for Personnel Security
Reviews

This memorandum is intended to update the EOP Security Office regarding those individuals authorized to review or process FBI background investigation files on behalf of the National Security Council. This memorandum also constitutes authorization for these same individuals to access information that may be relevant to security or suitability judgments regarding NSC employees, prospective employees, and detailees (hereinafter collectively employees) that derives from agencies other than the FBI.

In addition, this memorandum memorializes the understanding between the Office of White House Counsel and the National Security Council staff regarding the manner in which suitability judgments will be reached regarding NSC employees. Where matters potentially affecting suitability of NSC employees to work within the EOP complex are identified during review of Background Investigations or interviews with employees, the EOP Security Officer (or his designate) and the NSC Security Officer, shall bring such matters to the attention of the NSC/Legal Adviser or a Deputy Legal Adviser. The NSC may subsequently consult with the Office of White House Counsel on matters involving suitability as necessary to ensure that NSC employees are treated with the same rigor and in accord with the same standards applied by the White House generally. It is understood that subsequent to such consultation final decisions on suitability shall be taken by the NSC. Security clearances will continue to be adjudicated and/or confirmed by the NSC.

Consistent with this process, it is understood that where the NSC has favorably adjudicated an employee's suitability and security clearance, the employee shall receive a permanent pass unless a separate independent basis exists for not doing so; e.g., the employee poses a threat to the President, or has failed the drug test or tax check.

Reviewing or Processing FBI Background Investigation Files

The following individuals, whose signatures appear below, are authorized to review or process FBI and other agency background investigation files for the National Security Council. We understand, that by virtue of their positions, these persons are already authorized access to NSC background information. This memorandum is intended to confirm that access and to supplement those authorizations previously provided. With the exception of Ms. Haines and Mr. Hall, the individuals listed below require access on a periodic basis only. It is also understood that where Counter Intelligence concerns are raised, the NSC's Senior Director for Intelligence and/or his designate may be apprised of BI information.

The below Office of White House Counsel (OWHC) signatures shall also provide distinct authorization for OWHC access to the same information.

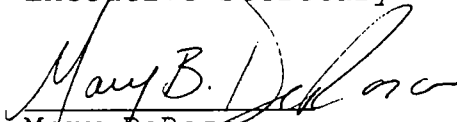
NSC



James Steinberg
Deputy Assistant to the President
for National Security Affairs

Donald L. Kerrick
Deputy Assistant to the President
for National Security Affairs

Glyn T. Davies
Executive Secretary

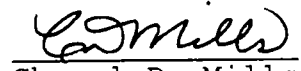


Mary DeRosa
Deputy Legal Adviser

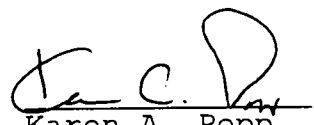
OWHC



Charles F.C. Ruff
Counsel to the President



Cheryl D. Mills
Deputy Counsel



Karen A. Popp
Associate Counsel

The following persons should be deleted from the previous NSC access list:

Alan Kreczko
John E. Sparks
Anthony Lake
Nancy E. Soderberg
Andrew D. Sens
Peter Erichsen

Concurrence by: Karen Popp ^{so 26}

Attachment
Tab A Previous NSC Authorization

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

60135

MEMORANDUM FOR CHARLES C. EASLEY
Director White House Security

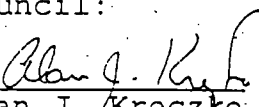
FROM: ANDREW D. SENS *AS*

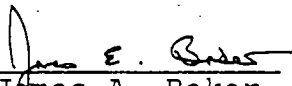
SUBJECT: Authorization for Personnel Security Reviews

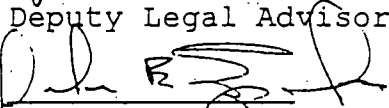
Consistent with the EOP's new Personnel Security procedures this memorandum is intended to notify the EOP Security Office of those individuals authorized to 1) approve the initiation of name checks and background investigations and 2) review or process FBI background investigation files on behalf of the National Security Council.

Approving Name Checks and Background Investigations

The following individuals, whose signatures appear below, are authorized to approve the initiation of name checks and background investigations on behalf of the National Security Council:


Alan J. Kreczko
Special Asst to the President
Legal Advisor, NSC


James A. Baker
Deputy Legal Advisor, NSC


John E. Sparks
Deputy Legal Advisor, NSC

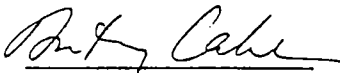
Reviewing or Processing FBI Background Investigation Files

The following individuals, whose signatures appear below, are authorized to review or process (i.e., physically handle and possess) FBI and other agency background investigation files for the National Security Council.

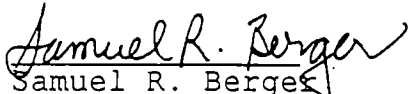
With the exception of Ms. Haines and Mr. Hall, the individuals listed below require access on an aperiodic basis only. In addition to reviewing information that may pertain to the suitability and clearance of NSC staff or prospective staff, the

Assistant to the President for National Security Affairs (APNSA), Deputy Assistants to the President for National Security Affairs (DAPNSAs), and representatives of the Office of the Legal Adviser are also asked by the White House Counsel and Presidential Personnel to evaluate information contained in the background files of prospective presidential appointees, where such information may implicate national security or foreign relations equities. Toward this end, the APNSA and DAPNSAs may determine that it is necessary to consult with additional NSC staff (not listed below) with specialized regional or functional knowledge. In such cases, additional NSC staff having access to FBI background information will be advised that such access is provided for official purposes only and such information shall be used only for the purpose of the specific consultation in question.

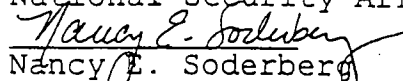
Finally, it should be noted that Mr. Leary, as the Senior Director for Records and Access Management, is authorized access and to possess background files and information to the extent required to perform his functions as Custodian of NSC records.



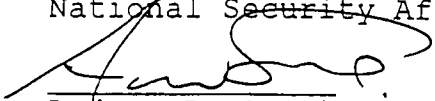
Anthony Lake
Asst to the President for
National Security Affairs



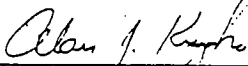
Samuel R. Berger
Dep Asst to the President for
National Security Affairs



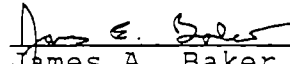
Nancy E. Soderberg
Dep Asst to the President for
National Security Affairs



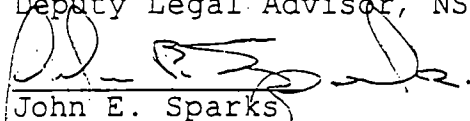
Andrew D. Sens
Executive Secretary, NSC



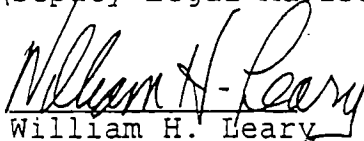
Alan J. Kreczko
Special Asst to the President
Legal Advisor, NSC



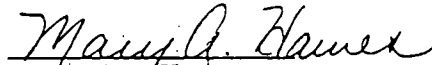
James A. Baker
Deputy Legal Advisor, NSC



John E. Sparks
Deputy Legal Advisor, NSC



William H. Leary
Senior Director for
Records & Access Management,
NSC



Mary A. Haines
Dir of Administration, NSC



James A. Hall
Security Officer, NSC

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

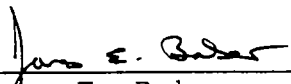
20006

MEMORANDUM FOR CHARLES C. EASLEY

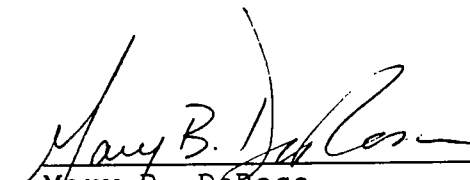
FROM: GLYN T. DAVIES

SUBJECT: Authorization for Initiation of Name Checks and
BI Investigations

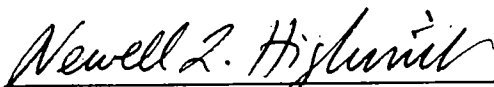
Consistent with the EOP's Personnel Security procedure, the following individuals, whose signatures appear below, are authorized to approve the initiation of name checks and background investigations on behalf of the National Security Council:



James E. Baker
Special Assistant to the
President and
Legal Adviser, NSC



Mary B. DeRosa
Deputy Legal Adviser, NSC



Newell L. Highsmith
Deputy Legal Adviser, NSC

NATIONAL SECURITY COUNCIL

WASHINGTON, D.C. 20506

May 4, 1994

INFORMATION

MEMORANDUM FOR ANTHONY LAKE

THROUGH: ALAN KRECZKO *AK*
FROM: JAMES BAKER *JB*
SUBJECT: DeConcini Talking Points Re: NSC Security

You asked for some talking points you could use with Senator DeConcini regarding security at the NSC. While NSC's record is not perfect, we are not aware of systematic problems regarding clearances or access to information regarding NSC staff (we do not address the EQP more generally). All personnel assigned to the NSC holding temporary or permanent passes have TS/SCI clearances. Persons awaiting clearance are not given access to the NSC computer system or permitted unrestricted access to classified work spaces.

In one instance, classified information was provided to a senior White House employee who did not hold the appropriate security clearance. Specifically, Phil Lader was kept on distribution for Roy Neel's NID. At the time, Lader held a TS clearance, but without SCI access. When this was realized in March, Lader was withdrawn from NID distribution until he was read into SCI. We also understand that you and Sandy Berger were not formally briefed on SCI access until March of this year. In addition, we cannot be certain that in the past year classified information originated by the NSC staff or Sit Room has not been passed to White House employees who were not appropriately cleared. We are not aware, however, that any information has been compromised and the Sit Room staff has been reminded to verify clearances before distributing information to White House employees no matter how senior.

Your talking points address the NSC situation only. If raised, you should inform DeConcini that WH security generally is being handled by WH Counsel. (DeConcini has an outstanding letter into Cutler on this.)

Concurrences by: George Tenet, Ralph Sigler, Bob Manzanare:

JB

Attachment

Tab I Talking Points

POINTS TO BE MADE FOR
TELEPHONE CONVERSATION WITH
SENATOR DECONCINI

- I share the importance you attach to information security. I sense, however, that you may have been left with the impression that there is a problem with NSC security. There is no such problem.
- All personnel assigned to the NSC who have access to classified information or unrestricted access to work spaces containing classified information hold TOP SECRET clearances with SCI access. They are subject to the same rules and requirements governing access to classified information applicable to all government employees. Persons pending assignment to the NSC who do not already have TS/SCI clearance may not access the NSC computer system or enter secure areas unaccompanied.
- That is not to say the NSC has been perfect. We have appropriate security procedures in place, although on occasion employees may not observe them. We are, however, re-emphasizing the importance of adherence to these procedures, which overall has been good.

C. 100

NATIONAL SECURITY COUNCIL

WASHINGTON, D.C. 20506

May 6, 1994

MEMORANDUM FOR MARVIN KRISLOV

FROM: JAMES BAKER⁵⁰

SUBJECT: NSC Personnel with White House and EOB Passes

The NSC's Administrative Office, including the Security Officer, has reviewed the list of names assigned against the NSC roll by the White House Security Office. The list of names is hand-dated May 5, 1994. I have reviewed the list as well.

Part of the confusion appears to stem from persons who are "dual-hatted," who are with the National Economic Council, but also carry NSC responsibilities in the area of international economic affairs. Some of these persons are counted on NSC's rolls and some are counted as NEC and do not count against the NSC's authorized strength of 151. Generally, detailees are carried by NSC, but there is no intuitive rule.

The more fundamental problem appears to be that the attached list, on which the White House Security Office is relying, is not accurate. Eight persons assigned to the NSC staff are not listed, including three Special Assistants to President (Bell, Claussen and Rosner). Thirteen other persons have already departed the NSC staff and 24 persons are, from NSC's perspective, attributable to other organizations or EOP offices, e.g., NARA, OSTP. Finally, the Assistant and Deputy Assistant to the President for National Security Affairs are considered White House employees, notwithstanding their obvious responsibilities regarding the NSC staff.

For NSC's part, we will continue to endeavor to keep the White House Security Office informed of NSC departure's and assignments. Our Administrative office is also available to work with the White House Security Office to identify specific employees assigned to the NSC rolls and those assigned elsewhere in the Old Executive Office Building. For your immediate purposes I recommend the following text (parentheticals are FYI): "As of May 4, there were 143 persons detailed to or employed by the National Security Council staff. Of this number:

- 65 held Permanent White House passes (Blue)(including one Other Government Agency pass);
- 45 held Temporary White House passes (Blue);
- 24 held Permanent EOB passes (Orange);
- 9 held Temporary EOB passes (Orange).

In addition, as of May 4 three contractors held Temporary White House passes in order to provide for training and maintenance on the NSC's computer systems. (FYI: Two of these contractors with

access to the computer system hold TS/SCI clearances. The third, who is working on a training manual and does not have access to the computer or unrestricted office access, does not.) Finally, and on occasion, anywhere from 2-10 executive branch employees may be loaned to the Executive Office of the President to work with the NSC staff on special projects, for example, to assist with document review and production in especially large cases." The next paragraph should also be modified to reflect the breakdown presented above. Thus, the topic sentence of the second paragraph should read: "All NSC employees, or persons utilizing NSC workspaces on an unrestricted basis, with permanent or temporary White House or Old Executive Office Building passes hold a Top Secret clearance with SCI access. . . ."

Please let me know if you have any questions regarding this information or the attachments. Thank you.

Concurrences: Bob Manzan^{ba}añares

Attachments

Tab A List of Names, 5/4/94.
 Tab B Memorandum from Security Officer Patricia Nelson.
 Tab C Draft Q and A, 4/28/JEB.

7/11/77

Bob Bell - *WHL*

WHL

Eileen Clausen-*WHL*

Edwards, Joan.

- OCHA

WHL

OSTP

Amsstrong

SSDS contractor

NEC

ANDREASEN	STEVEN	PETER	621 58457	TWHS
ANDRICOS	GEORGE	MICHAEL	621 49462	WHS
AOKI	STEVEN		621 59177	TWHS
ARGARIN	JOCELYN	DERIGUITO	621 56740	WHS
ATLAS	EDWIN	LINDSAY	621 59989	TWHS
BAILEY	DAVID	REX	621 57548	WHS
BAKER	JAMES	EDGAR	621 60659	TWHS
BAKER	JANE	ELIZABETH	621 52442	WHS
BAKKE	KYLE	DUANE	621 56860	WHS
BALDWIN	KENNETH		621 60340	TWHS
BATTENFIELD	PATRICIA	ANN	621 26851	EOB
BEERS	R. RAND		621 49897	TWHS
BELLAMY	RALPH	CARTER	621 24239	WHS
BERGER	SAMUEL	RICHARD	621 58185	TWHS
BEYRLE	JOHN	ROSS	621 60331	TWHS
BIEDA	JAMES	MICHAEL	621 57651	WHS
BLEICKEN	NEIL	GERHARD	621 55681	EOB
BLIEBERGER	MARION	HOLLOWAY	621 55864	TEO
BOLINSKI	CHARLENE	CONSTANCE	621 42725	EOB
BOYKIN	EVELYN	GENEE	621 60436	TEO
BRESNAHAN	GARY	EDWIN	621 36394	WHS
BROADWAY	JAMUNA	DEVI	621 61054	TEO
BRYAN	LLOYD	DAVID	621 59904	WHS
BURGUS	CARLOS	ANTONIO	621 59415	WHS
BURNS	R. NICHOLAS		621 53349	WHS
CANAS	RICHARD	LEON	621 53801	WHS
CHERN	KENNETH	STEPHEN	621 60795	TWHS
CHYBA	CHRISTOPHER	FRANK	621 60250	WHS
CICIO	KRISTEN	KAROL	621 50444	WHS
CLARK	BRONYA	HARTNESS	621 46056	EOB
CLARK	VICKI	MARIE	621 60841	TEO
CLARKE	RICHARD	ALAN	621 57586	WHS
CLEMENTS	WILLIAM	LAWRENCE	621 60024	TWHS
CLEVELAND	CARDLYN	ELIZABETH	621 30894	EOB
CONLEY	STEPHEN	CARROLL	621 48738	WHS
COOPER	KATHLEEN	HELEN	621 61077	TEO
CRISPELL	THOMAS	GLENN	621 58128	TWHS
DANIEL	PATTY	ANNALEE	621 50377	EOB
DANVERS	WILLIAM	CHAPPELL	621 60866	TWHS
DARBY	MELANIE	BROOKE	621 58264	WHS
DARRAGH	SEAN	JOSEPH	621 58178	WHS
DAVIS	JAMES	WASHINGTON	621 11368	WHS
DESHAZER	MACARTHUR		621 60607	WHS
DIMEL	MARSHA	LOUISE	621 57998	TWHS
DONOVAN	LINDA	MARIE	621 51122	TEO
DRAGONE	KAREN	DENISE	621 61159	TWHS
DURUY	SHAWN	LEE	621 60790	TEO
EMERY	MARY	CATHERINE	621 54250	WHS
FAOVER	ROBERT	CLARKE	621 58833	WHS

CFR	FEAVER	PETER	DOUGLAS	621 60174	TWHS
	FEINBERG	RICHARD	EDWARD	621 58378	WHS
	FICKLIN	JOHN	WRORY	621 28890	WHS
	FORSYTHE	ROSEMARIE	CRISOSTOMO	621 59281	WHS
	FRIED	DANIEL		621 60105	TWHS
Nec	FROMAN	MICHAEL	BRAVERMAN	621 57758	WHS
	FUNCHES	CHRISTINA	LAURELLE	621 49510	EOB
	GATES	BRIAN	KEITH	621 60640	TWHS
	GENTON	REGINA	ANN	621 60539	WHS
	GEORGE	CHRISTOPHER	LEE	621 35044	WHS
Armstrong	GLENN	SUZANNE	LAGRANGE	621 61101	TEO
	GOTTEMUELLER	ROSE	EILENE	621 58479	WHS
	GRAY	WENDY	ELAINE	621 47697	WHS
	HAHN	KEITH	DENNIS	621 57050	WHS
	HALL	WILMA	GRAY	621 25239	WHS
	HALPERIN	MURTON	H	621 60965	TWHS
	HAMMOND	LISA	WILLARD	621 61049	TEO
	HAMMONDS	D. HOLLY		621 50891	TWHS
	HARRIS	ELISA	DAVIDSON	621 58477	TWHS
	HEALEY	ELISABETH	ANNE	621 56754	WHS
	HERRINGTON	DAVID	EDWIN	621 57854	WHS
	HILL	ROSEANNE	MARIE	621 35237	EOB
	HILLIARD	BRENDA	IRONMONGER	621 46858	WHS
Armstrong	HOBSON	GEORGEANN	MARIE	621 61100	TEO
	HOLL	JANE	ELLEN	621 55943	WHS
Armstrong	HORN JR.	ARTHUR	WILLIAM	621 61112	TEO
	HOUCK	BAERBEL	KLARA	621 35050	EOB
	HUBER	FRANCIS	JOSEPH	621 55634	WHS
	INDYK	MARTIN	SEAN	621 58497	WHS
	ITOH	WILLIAM	HENRY	621 58360	TWHS
	JOHNSON	JAMES	MARK	621 53893	WHS
	JONES	JEFFREY	B	621 55626	WHS
	JONES	STEVEN	RAY	621 58469	WHS
	KELLY	SANDRA	L	621 31547	EOB
	KENNEY	KRISTIE	ANNE	621 58836	TWHS
	KERR	ANDREW	STANLEY	621 57903	WHS
	KRECZKO	ALAN	JAMES	621 59414	TWHS
	KRISTOFF	SANDRA	JEANNE	621 58828	TWHS
	KYLE	ROBERT	DIXON	621 58901	TWHS
	LAIPSON	ELLEN	BETH	621 60334	TWHS
	LAPLANTE	M. KAY		621 43880	WHS
	LEARY	WILLIAM	HENRY	621 56438	WHS
	LEBOURGEOIS	JULIEN	DUDLEY	621 60616	TWHS
	LINDSEY	WANDA	DENISE	621 52313	EOB
	LIU	ERIC	P	621 60649	TWHS
Student Intern	MANN	HILLARY	PRUDENCE	621 60537	TEO
	MANZANARES	JOSEPH	ROBERT	621 59561	WHS
	MARMOL	MADELYN	PAULA	621 60830	TWHS
	MARSHALL	BETTY	ANN	621 21858	EOB
	MAXFIELD	NANCY	HELENE	621 52140	EOB
	MCGEATH	TIMOTHY	ALAN	621 57641	WHS
	MCILHANY	JESTKA	ANAYANSI	621 59692	TEO

Hummerwald, Tom.
11/13

	MESHAHE	JOHN	FRANCIS	621 56358	WHS
	MERCHANT	BRIAN	TIMOTHY	621 28007	EOB
	MILLISON	CATHY	LOUISE	621 30613	WHS
	MISLOCK JR.	RAYMOND	ANTHONY	621 60898	TWHS
NSE	MITCHELL, III	CALVIN	ARTHUR	621 60745	TWHS
	MITSLER	ELAINE		621 45058	WHS
	MOODY	ANGELYN	DELOIS	621 35476	EOB
NSE	MURASE	EMILY	MOTO	621 60538	TEO
	MURPHY	MILES	RANDALL	621 56896	WHS
	NEIL	M ELISE		621 42903	EOB
	NELSON	PATRICIA	DEAN	621 46232	WHS
	NIEMERSKI	STEPHEN	GREGORY	621 57503	WHS
	NORMAN	MARCIA	GAIL	621 59416	TEO
	OLOUGHLIN	KATHERINE	ENGEL	621 57640	TWHS
	OWENS-KIRKPATR	DARBO	APPELQVIST	621 50834	WHS
	PAHLKE	HELEN		621 44862	WHS
	PARRAMORE	CARL	WAYNE	621 59971	WHS
	PEGGINS	JOHN	WALTER	621 50689	WHS
	PERROY	DEBORAH	WOOD	621 49789	EOB
	PETCHEL	BEVERLY	LORRAINE	621 44863	TEO
	PITMAN	JAMES	NORTON	621 59364	TWHS
	PONEMAN	DANIEL	BRUCE	621 54117	WHS
	PORTER	GIDELL		621 60342	WHS
	ROTT	CHRISTINE	LYNN	621 57373	EOB
	PUNKE	MICHAEL	WARD	621 58267	WHS
	QUINN	MARY	ELIZABETH	621 50676	EOB
	RAMSAY	MARTHA	SUE	621 55842	EOB
	REED	JAMES	WILLIAM	621 59369	TWHS
	RICE	SUSAN	ELIZABETH	621 58853	TWHS
	ROSS	THOMAS	BERNARD	621 61128	TWHS
	ROSSIN	LAWRENCE	GEORGE	621 59871	TWHS
	ROTH	STANLEY	OWEN	621 61092	TWHS
	SALVETTI	LISA	MARIE	621 53077	EOB
	SATTERFIELD	DAVID	MICHAEL	621 59376	TWHS
	SCHIFTER	RICHARD		621 60104	TWHS
	SCULIMBRENE	THOMAS	ANTHONY	621 49948	WHS
	SEELEY	CHARLOTTE	PALMER	621 53330	EOB
	SEVIGNY JR.	THEODORE	THOMAS	621 59377	WHS
	SHEEHAN	MICHAEL	ANDREW	621 52493	WHS
	SIGLER	RALPH	HOYT	621 22546	WHS
SOS Contractor	SIMONS	JAMES	ROBERT	621 60483	TEO
	SNOW	DIANA	LYNN	621 56097	EOB
Wt	SODERBERG	NANCY	ELIZABET	621 58186	WHS
	SONENSHINE	TARA	DIANE	621 60982	WHS
7-24	SPEIGHT	ERIC	LEE	621 60263	TEO
	SPENCER	WILLIAM	HALL	621 57772	TWHS
	STALCUP	RUTH		621 53149	EOB
	STAUFFER	HELEN	LOUISE	621 59381	TEO
	STEINBERG	DONALD	KENNETH	621 59712	TWHS
	SUETTINGER	ROBERT	LEE	621 61114	TWHS
Waco	SULSER	JACK	ARNOLD	621 50328	EOB

Rogers, Jimmy - JWH

NARA

TDY

CFR

TAPARRA	FIDEL	GENSON	621 50743	TEL
TENET	GEORGE	JOHN	621 58384	TWHS
TURNER	VERONICA	BERNARDINE	621 60794	TEL
TURNER III	JOE	THORNTON	621 60002	TWHS
VANTASSEL	DAVID	STERLING	621 58275	WHS
VEIT	KATHY	MARIE	621 58690	WHS
WADDELL	RICKY	LYNN	621 60793	WHS
WADSWORTH	VALON	JAY	621 58471	WHS
WALKER	JENONNE	R	621 58375	TWHS
WALLACK	MATTHEW	DOUGLAS	621 60780	TWHS
WALSH	HELEN	CLAIRE	621 57692	WHS
WIEDEMANN	KENT	MANS	621 58839	WHS
WILSON	MARILYN	EUNICE	621 51694	EOB
WILSON III	ERNEST	JAMES	621 58458	WHS
WITKOWSKY	ANNE	ADAMS	621 58459	TWHS
WOLIN	NEAL	STEVEN	621 59370	WHS
WRIGHT	ALLISON	MARIE	621 58987	WHS
ZULEWSKI	RICHARD	A	621 61071	TEL

TOTAL EMPLOYEES FOR NATIONAL SECURITY COUN =

172

14
24
88

Hawkins, Ardenia

TWHS
65
PWHS
64

FLECH
24
TEL
9

54-Temp
88-Farm
11-1-1961

Whymann, William
Wooten, Kevin
Wozniak, Nabahi
FTH SSOS contractor

Nelson, Patricia D.

To: Manzanares
Subject: Passes

Bob,

There's 172 personnel assigned against the NSC roll. There are 8 personnel who were left off the roster. The following is a break down of those personnel:

- 2 not NSC personnel (WH)
- 13 departed the NSC
- 3 SSDS contractors
- 1 WH Fellow
- 4 Armstrong Case
- 4 NEC
- 4 NARA
- 2 CFR
- 1 OSTP
- 1 Student Intern
- 2 TDYs

Out of a total of 180, 37 (above) are not NSC, leaving a total of 143.

Out of the 143, there are 45 TWHS passes, 9 TEO, 64 PWHS, 24 PEO and 1 OGA. *blue*

There's a total of 54 Temp passes and 89 Perm passes, Total: 143

Q. Have any temporary passes been issued for personnel assigned to work for the National Security Council (NSC), or who frequent work spaces occupied by the staff of the NSC?

A. Yes. As of April 26, 151 persons were detailed to, employed by, or pending assignment to the National Security Council staff. Of this number, 104 had permanent passes and 44 had temporary passes. The remainder represent positions in the process of being filled. In addition, on occasion anywhere from 2-10 executive branch employees may be loaned to the Executive Office of the President (EOP) and NSC staff to work on special projects, e.g., to assist with document review and production in especially large cases.

All NSC employees, or persons utilizing NSC workspaces, with permanent or temporary White House passes hold a TOP SECRET clearance with SCI access. NSC employees awaiting security clearances, persons pending assignment to the NSC staff, or any other government persons who do not hold TS/SCI clearance may not access the NSC computer system or enter secure areas unaccompanied. In addition, the White House Situation Room receives certification of clearances before permitting NSC employees access to national security information they have a need to know.

Because White House employees are subject to security and suitability reviews beyond those required of other executive branch employees, there are occasions where NSC staff may hold a TOP SECRET clearance with SCI access, but not yet be eligible for a permanent pass. This would occur, for example, when an NSC employee has not had an updated background investigation within one year of joining the EOP. Agencies typically require updated background investigations every five years, however, to work at the White House, a background investigation must have been completed within one year of an employee joining the EOP.

In addition, NSC employees are also subject to the suitability review required of all EOP employees as discussed above. Until such time as a suitability review and updated background investigation is completed (if necessary), a permanent pass will not be issued to NSC employees.

Q. Have all personnel assigned to the NSC, or who frequent the work spaces occupied by the staff of the NSC, completed their background investigations?

As noted above, all personnel assigned to the NSC who have access to classified information or work spaces containing classified information hold TOP SECRET clearances with SCI access. In instances where an employee holds such a clearance, but is required to undergo an updated background investigation for the purpose of complying with the EOP's one-year rule, an employee will be given access to classified information while this updated background investigation is pending. This procedure permits the work of the NSC to continue unabated while safeguarding national security information.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

January 5, 1998

ACTION

MEMORANDUM FOR DONALD L. KERRICK 

FROM:

JAMES BAKER 

SUBJECT:

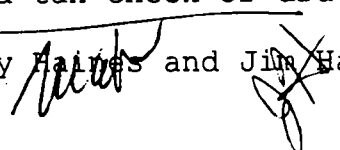
Access to NSC Background Investigations & Process
for NSC Suitability Determinations

The White House Security Office has requested a revised list of persons authorized access to FBI background materials on NSC personnel. The attached memorandum from Glyn Davies provides such an update.

The memorandum also memorializes the process by which the NSC, in consultation with the Office of White House Counsel, will make suitability determinations. In reaching this formulation we considered carefully whether such decisions should ultimately be made by the White House Counsel or the NSC. Counsel's Office argued that if they were to serve as ultimate arbiter of suitability, WHC rather than NSC, should make all the NSC's suitability determinations and not just those in the difficult cases we raise. As a result, we recommend the formula above: NSC in consultation with WHC. This will allow the NSC to control the tempo of its own security and suitability decisions and is, I believe, consistent with the Front Office's own view that the APNSA ultimately should decide who works on the NSC staff.

The NSC Security Officer will continue to adjudicate, or verify, access to national security information for NSC staff using the standards contained in E.O. 12968 and corresponding adjudicative guidelines. The Secret Service will continue to evaluate employees from the perspective of potential threats to the President. The Office of White House Security will continue to serve as gatekeeper for BI requests and ensure the necessary steps have been taken before issuance of a permanent pass. However, as the attached memorandum underscores, where the NSC has favorably adjudicated security and suitability, a permanent pass will be issued unless there is a separate basis for denying access, such as a failed tax check or drug test.

Concurrence by:

Mary Haines and Jim Hall 

RECOMMENDATION

That you and Glyn sign the attached signature page and that you authorize Glyn Davies to sign the memorandums at Tabs I and II.

Approve ✓ Disapprove

Attachments

Tab I Memorandum for Chuck Easley Re Authorization
for Review or Process BI Files for NSC

Tab A Prior NSC Authorization for BI Access

Tab II Memorandum for Chuck Easley Re Approval and
Initiation of BI Access for NSC

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

20006

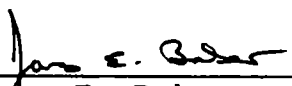
January 13, 1998

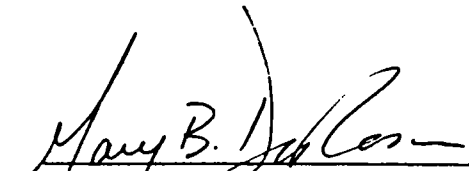
MEMORANDUM FOR CHARLES C. EASLEY

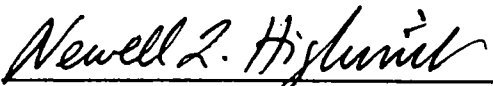
FROM: GLYN T. DAVIES 

SUBJECT: Authorization for Initiation of Name Checks and
BI Investigations

Consistent with the EOP's Personnel Security procedure, the following individuals, whose signatures appear below, are authorized to approve the initiation of name checks and background investigations on behalf of the National Security Council:


James E. Baker
Special Assistant to the
President and
Legal Adviser, NSC


Mary B. DeRosa
Deputy Legal Adviser, NSC


Newell L. Highsmith
Deputy Legal Adviser, NSC

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

20006

January 13, 1998

MEMORANDUM FOR CHARLES C. EASLEY

FROM:

GLYN DAVIES *GD*

SUBJECT:

Updated Authorization for Personnel Security
Reviews

This memorandum is intended to update the EOP Security Office regarding those individuals authorized to review or process FBI background investigation files on behalf of the National Security Council. This memorandum also constitutes authorization for these same individuals to access information that may be relevant to security or suitability judgments regarding NSC employees, prospective employees, and detailees (hereinafter collectively employees) that derives from agencies other than the FBI.

In addition, this memorandum memorializes the understanding between the Office of White House Counsel and the National Security Council staff regarding the manner in which suitability judgments will be reached regarding NSC employees. Where matters potentially affecting suitability of NSC employees to work within the EOP complex are identified during review of Background Investigations or interviews with employees, the EOP Security Officer (or his designate) and the NSC Security Officer, shall bring such matters to the attention of the NSC/Legal Adviser or a Deputy Legal Adviser. The NSC may subsequently consult with the Office of White House Counsel on matters involving suitability as necessary to ensure that NSC employees are treated with the same rigor and in accord with the same standards applied by the White House generally. It is understood that subsequent to such consultation final decisions on suitability shall be taken by the NSC. Security clearances will continue to be adjudicated and/or confirmed by the NSC.

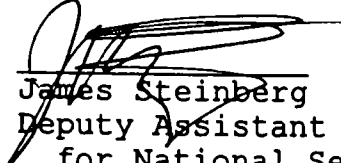
Consistent with this process, it is understood that where the NSC has favorably adjudicated an employee's suitability and security clearance, the employee shall receive a permanent pass unless a separate independent basis exists for not doing so; e.g., the employee poses a threat to the President, or has failed the drug test or tax check.

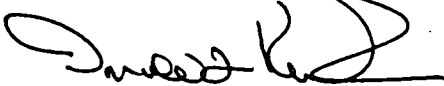
Reviewing or Processing FBI Background Investigation Files

The following individuals, whose signatures appear below, are authorized to review or process FBI and other agency background investigation files for the National Security Council. We understand, that by virtue of their positions, these persons are already authorized access to NSC background information. This memorandum is intended to confirm that access and to supplement those authorizations previously provided. With the exception of Ms. Haines and Mr. Hall, the individuals listed below require access on a periodic basis only. It is also understood that where Counter Intelligence concerns are raised, the NSC's Senior Director for Intelligence and/or his designate may be apprised of BI information.

The below Office of White House Counsel (OWHC) signatures shall also provide distinct authorization for OWHC access to the same information.

NSC

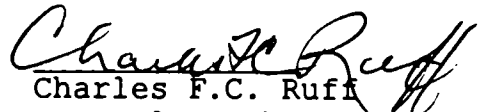

James Steinberg
Deputy Assistant to the President
for National Security Affairs


Donald L. Kerrick
Deputy Assistant to the President
for National Security Affairs

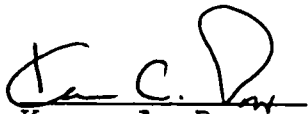

Glyn T. Davies
Executive Secretary


Mary DeRosa
Deputy Legal Adviser

OWHC


Charles F.C. Ruff
Counsel to the President


Cheryl D. Mills
Deputy Counsel


Karen A. Popp
Associate Counsel

The following persons should be deleted from the previous NSC access list:

Alan Kreczko
John E. Sparks
Anthony Lake
Nancy E. Soderberg
Andrew D. Sens
Peter Erichsen

Concurrence by: ^{so 26} Karen Popp

Attachment
Tab A Previous NSC Authorization

MEMORANDUM FOR CHARLES C. EASLEY
Director White House Security

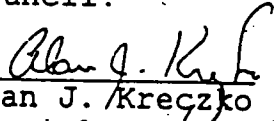
FROM: ANDREW D. SENS *AS*

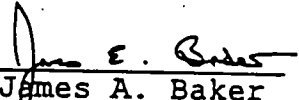
SUBJECT: Authorization for Personnel Security Reviews

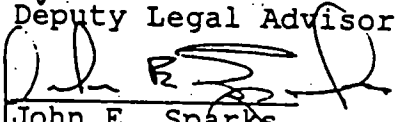
Consistent with the EOP's new Personnel Security procedures this memorandum is intended to notify the EOP Security Office of those individuals authorized to 1) approve the initiation of name checks and background investigations and 2) review or process FBI background investigation files on behalf of the National Security Council.

Approving Name Checks and Background Investigations

The following individuals, whose signatures appear below, are authorized to approve the initiation of name checks and background investigations on behalf of the National Security Council:


Alan J. Kreczko
Special Asst to the President
Legal Advisor, NSC


James A. Baker
Deputy Legal Advisor, NSC


John E. Sparks
Deputy Legal Advisor, NSC

Reviewing or Processing FBI Background Investigation Files

The following individuals, whose signatures appear below, are authorized to review or process (i.e., physically handle and possess) FBI and other agency background investigation files for the National Security Council.

With the exception of Ms. Haines and Mr. Hall, the individuals listed below require access on an aperiodic basis only. In addition to reviewing information that may pertain to the suitability and clearance of NSC staff or prospective staff, the

Assistant to the President for National Security Affairs (APNSA), Deputy Assistants to the President for National Security Affairs (DAPNSAs), and representatives of the Office of the Legal Adviser are also asked by the White House Counsel and Presidential Personnel to evaluate information contained in the background files of prospective presidential appointees, where such information may implicate national security or foreign relations equities. Toward this end, the APNSA and DAPNSAs may determine that it is necessary to consult with additional NSC staff (not listed below) with specialized regional or functional knowledge. In such cases, additional NSC staff having access to FBI background information will be advised that such access is provided for official purposes only and such information shall be used only for the purpose of the specific consultation in question.

Finally, it should be noted that Mr. Leary, as the Senior Director for Records and Access Management, is authorized access and to possess background files and information to the extent required to perform his functions as Custodian of NSC records.

Anthony Lake

Anthony Lake
Asst to the President for
National Security Affairs

Samuel R. Berger

Samuel R. Berger
Dep Asst to the President for
National Security Affairs

Nancy E. Soderberg

Nancy E. Soderberg
Dep Asst to the President for
National Security Affairs

Andrew D. Sens

Andrew D. Sens
Executive Secretary, NSC

Alan J. Kreczko

Alan J. Kreczko
Special Asst to the President
Legal Advisor, NSC

James A. Baker

James A. Baker
Deputy Legal Advisor, NSC

John E. Sparks

John E. Sparks
Deputy Legal Advisor, NSC

William H. Leary

William H. Leary
Senior Director for
Records & Access Management,
NSC

Mary A. Haines

Mary A. Haines
Dir of Administration, NSC

James A. Hall

James A. Hall
Security Officer, NSC

NATIONAL SECURITY COUNCIL
DISTRIBUTION RECEIPT

LOG 9820006
DATE 13 JAN 98

SUBJECT: AUTHORIZATION FOR INITIATION OF NAME CHECKS & BI INVESTIGATIONS
DOCUMENT CLASSIFICATION: UNCLASSIFIED

EXTERNAL DISTRIBUTION:

DATE

TIME

SIGNATURE

EASLEY, C
4013 NEOB
EOP SECURITY

PRINT LAST NAME: _____

COPY: ORIGINAL

DATE, TIME, SIGN THE RECEIPT AND RETURN TO: NSC RECORDS MGNT. ROOM 379 OEOB

PAGE 01 OF 01 PAGES

UNCLASSIFIED
NSC/RMO PROFILE

RECORD ID: 9820006
RECEIVED: 05 JAN 98 14

TO: EASLEY, C

FROM: DAVIES

DOC DATE: 13 JAN 98
SOURCE REF:

KEYWORDS: ADMINISTRATIVE
LEGAL ISSUES

SECURITY

PERSONS:

SUBJECT: AUTHORIZATION FOR INITIATION OF NAME CHECKS & BI INVESTIGATIONS

ACTION: DAVIES SGD MEMO

DUE DATE: 08 JAN 98 STATUS: C

STAFF OFFICER: BAKER

LOGREF:

FILES: NS

NSCP:

CODES:

DOCUMENT DISTRIBUTION

FOR ACTION

FOR CONCURRENCE

FOR INFO

BAKER
HAINES
HALL
NSC CHRON

COMMENTS:

DISPATCHED BY

DRS / CIG

DATE

1/14

BY HAND

W/ATTCH

OPENED BY: NSJWF

CLOSED BY: NSDRS

DOC 3 OF 3

UNCLASSIFIED

UNCLASSIFIED
ACTION DATA SUMMARY REPORT

RECORD ID: 9820006

DOC ACTION OFFICER

CAO ASSIGNED ACTION REQUIRED

001 KERRICK	Z 98010821 FOR DECISION
001	X 98010917 KERRICK APPROVED RECOM
001 BAKER	X 98011013 FOR FURTHER ACTION
002	X 98011317 DAVIES SGD MEMO
003	X 98011317 DAVIES SGD MEMO

DISPATCH DATA SUMMARY REPORT

DOC DATE DISPATCH FOR ACTION

DISPATCH FOR INFO

002	980113	EASLEY, C
003	980113	EASLEY, C

UNCLASSIFIED

National Security Council
The White House

PROOFED BY: _____ LOG # 20006
URGENT NOT PROOFED: _____ SYSTEM PRS NSO INT ARS
BYPASSED WW DESK: _____ DOCLOG 6WY A/O _____

	SEQUENCE TO	INITIAL/DATE	DISPOSITION
Cosgriff	_____	_____	_____
Rice	<u>1</u>	<u>② 1/12</u>	_____
Davies	<u>2</u>	<u>② 1/12</u>	_____
Kerrick	_____	_____	_____
Steinberg	_____	_____	_____
Berger	_____	_____	_____
Situation Room	_____	_____	_____
West Wing Desk	<u>3</u>	<u>② 1/13</u>	<u>DJ</u>
Records Mgt.	<u>4</u>	_____	<u>N</u>
_____	_____	_____	_____

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

cc:

COMMENTS: Need Davies signatures @
Tab I p. 2 & Tab II.
Done

38 JAN 12 PM 4:03

Exec Sec Office has diskette YD

National Security Council
The White House

PROOFED BY: _____ LOG # 20006
URGENT NOT PROOFED: _____ SYSTEM PRS (NSC) INT ARS
BYPASSED WW DESK: _____ DOCLOG (7) A/O _____

	SEQUENCE TO	INITIAL/DATE	DISPOSITION
<i>UP</i> Cosgriff			
Rice	<u>1</u>		
Davies	<u>1</u>	<u>G 1/8</u>	
Kerrick	<u>2</u>	<u>(K)</u>	
Steinberg			
Berger			
Situation Room			
West Wing Desk	<u>3</u>	<u>(TE) 1/9</u>	<u>STAFF</u>
Records Mgt.			
<u>Baker</u>	<u>4</u>		<u>See OTD Note</u>

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

cc:

COMMENTS:

98 JAN 8 PM 8:07

Exec Sec Office has diskette yes

Handwritten:
JL
Does this mean
the SRB does not
have access? (2)
So, we need
to think
about that? (2)