Department of Defense
DIRECTIVE

This version of DoD Directive 5220.6 contains the Revised Adjudicative Guidelines implemented for the Department of Defense by the Undersecretary of Defense for Intelligence on August 30, 2006 and made effective for any adjudication in which a Statement of Reasons issued on or after September 1, 2006.

NUMBER 5220.6
January 2, 1992

Administrative Reissuance Incorporating Through Change 4, April 20, 1999
GC, DoD

SUBJECT: Defense Industrial Personnel Security Clearance Review Program

References: (a) DoD Directive 5220.6, subject as above, August 12, 1985 (hereby canceled)
(b) DoD 5200.2-R, "Department of Defense Personnel Security Program," January 1987, authorized by DoD Directive 5200.2, December 20, 1979
(c) Section 1001 of title 18, United States Code
(d) Section 101 et seq. of title 28, United States Code

1. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update policy, responsibilities, and procedures of the Defense Industrial Personnel

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Inspector General of the Department of Defense (IG, DoD), and the Defense Agencies (hereafter referred to collectively as "the DoD Components").

2.2. By mutual agreement, also extends to other Federal Agencies that include:

2.2.1. Department of Agriculture.

2.2.2. Department of Commerce.

2.2.3. Department of Interior.

2.2.4. Department of Justice.

2.2.5. Department of Labor.

2.2.6. Department of State.

2.2.7. Department of Transportation.

2.2.8. Department of Treasury.

2.2.9. Environmental Protection Agency.

2.2.10. Federal Emergency Management Agency.

2.2.11. Federal Reserve System.

2.2.12. General Accounting Office.

2.2.13. General Services Administration.

2.2.14. National Aeronautics and Space Administration.

2.2.15. National Science Foundation.

2.2.16. Small Business Administration.

2.2.17. United States Arms Control and Disarmament Agency.

2.2.18. United States Information Agency.

2.2.19. United States International Trade Commission.

2.2.20. United States Trade Representative.

2.3. Applies to cases that the Defense Industrial Security Clearance Office (DISCO) forwards to the Defense Office of Hearings and Appeals (DOHA), Defense Legal Services Agency for action under this Directive to determine whether it is clearly

consistent with the national interest to grant or continue a security clearance for the applicant.

2.4. Provides a program that may be extended to other security cases at the direction of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)).

2.5. Does not apply to cases in which:

2.5.1. A security clearance is withdrawn because the applicant no longer has a need for access to classified information;

2.5.2. An interim security clearance is withdrawn by the DISCO during an investigation; or

2.5.3. A security clearance is withdrawn for administrative reasons that are without prejudice as to a later determination of whether the grant or continuance of the applicant's security clearance would be clearly consistent with the national interest.

2.6. Does not apply to cases for access to sensitive compartmented information or a special access program.

3. DEFINITIONS

3.1. Applicant. Any U.S. citizen who holds or requires a security clearance or any immigrant alien who holds or requires a limited access authorization for access to classified information needed in connection with his or her employment in the private sector; any U.S. citizen who is a direct-hire employee or selectee for a position with the North Atlantic Treaty Organization (NATO) and who holds or requires NATO certificates of security clearance or security assurances for access to U.S. or foreign classified information; or any U.S. citizen nominated by the Red Cross or United Service Organizations for assignment with the Military Services overseas. The term "applicant" does not apply to those U.S. citizens who are seconded to NATO by U.S. Departments and Agencies or to U.S. citizens recruited through such Agencies in response to a request from NATO.

3.2. Clearance Decision. A decision made in accordance with this Directive concerning whether it is clearly consistent with the national interest to grant an applicant a security clearance for access to Confidential, Secret, or Top Secret information. A favorable clearance decision establishes eligibility of the applicant to

be granted a security clearance for access at the level governed by the documented need for such access, and the type of investigation specified for that level in DoD 5200.2-R (reference (b)). An unfavorable clearance decision denies any application for a security clearance and revokes any existing security clearance, thereby preventing access to classified information at any level and the retention of any existing security clearance.

4. POLICY

It is DoD policy that:

4.1. All proceedings provided for by this Directive shall be conducted in a fair and impartial manner.

4.2. A clearance decision reflects the basis for an ultimate finding as to whether it is clearly consistent with the national interest to grant or continue a security clearance for the applicant.

4.3. Except as otherwise provided for by E.O. 10865 (enclosure 1) or this Directive, a final unfavorable clearance decision shall not be made without first providing the applicant with:

4.3.1. Notice of specific reasons for the proposed action.

4.3.2. An opportunity to respond to the reasons.

4.3.3. Notice of the right to a hearing and the opportunity to cross-examine persons providing information adverse to the applicant.

4.3.4. Opportunity to present evidence on his or her own behalf, or to be represented by counsel or personal representative.

4.3.5. Written notice of final clearance decisions.

4.3.6. Notice of appeal procedures.

4.4. Actions pursuant to this Directive shall cease upon termination of the applicant's need for access to classified information except in those cases in which:

4.41. A hearing has commenced.

4.4.2. A clearance decision has been issued; or

4.4.3. The applicant's security clearance was suspended and the applicant provided a written request that the case continue.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

5.1.1. Establish investigative policy and adjudicative standards and oversee their application.

5.1.2. Coordinate with the General Counsel of the Department of Defense (GC, DoD) on policy affecting clearance decisions.

5.1.3. Issue clarifying guidance and instructions as needed.

5.2. The General Counsel of the Department of Defense shall:

5.2.1. Establish guidance and provide oversight as to legal sufficiency of procedures and standards established by this Directive.

5.2.2. Establish the organization and composition of the DOHA.

5.2.3. Designate a civilian attorney to be the Director, DOHA.

5.2.4. Issue clarifying guidance and instructions as needed.

5.2.5. Administer the program established by this Directive.

5.2.6. Issue invitational travel orders in appropriate cases to persons to appear and testify who have provided oral or written statements adverse to the applicant relating to a controverted issue.

5.2.7. Designate attorneys to be Department Counsels assigned to the DOHA to represent the Government's interest in cases and related matters within the applicability and scope of this Directive.

5.2.8. Designate attorneys to be Administrative Judges assigned to the DOHA.

5.2.9. Designate attorneys to be Administrative Judge members of the DOHA Appeal Board.

5.2.10. Provide for supervision of attorneys and other personnel assigned or attached to the DOHA.

5.2.11. Develop and implement policy established or coordinated with the GC, DoD, in accordance with this Directive.

5.2.12. Establish and maintain qualitative and quantitative standards for all work by DOHA employees arising within the applicability and scope of this Directive.

5.2.13. Ensure that the Administrative Judges and Appeal Board members have the requisite independence to render fair and impartial decisions consistent with DoD policy.

5.2.14. Provide training, clarify policy, or initiate personnel actions, as appropriate, to ensure that all DOHA decisions are made in accordance with policy, procedures, and standards established by this Directive.

5.2.15. Provide for maintenance and control of all DOHA records.

5.2.16. Take actions as provided for in subsection 6.2., below, and the additional procedural guidance in enclosure 3.

5.2.17. Establish and maintain procedures for timely assignment and completion of cases.

5.2.18. Issue guidance and instructions, as needed, to fulfill the foregoing responsibilities.

5.2.19. Designate the Director, DOHA to implement paragraphs 5.2.5. through 5.2.18., above, under general guidance of the GC, DoD.

5.3. The Heads of the DoD Components shall provide (from resources available to the designated DoD Component) financing, personnel, personnel spaces, office facilities, and related administrative support required by the DOHA.

5.4. The ASD(C3I) shall ensure that cases within the scope and applicability of this Directive are referred promptly to the DOHA, as required, and that clearance decisions by the DOHA are acted upon without delay.

6. PROCEDURES

6.1. Applicants shall be investigated in accordance with the standards in DoD 5200.2-R (reference (b)).

6.2. An applicant is required to give, and to authorize others to give, full, frank, and truthful answers to relevant and material questions needed by the DOHA to reach a clearance decision and to otherwise comply with the procedures authorized by this Directive. The applicant may elect on constitutional or other grounds not to comply; but refusal or failure to furnish or authorize the providing of relevant and material information or otherwise cooperate at, any stage in the investigation or adjudicative process may prevent the DOHA from making a clearance decision. If an applicant fails or refuses to:

6.2.1. Provide relevant and material information or to authorize others to provide such information; or

6.2.2. Proceed in a timely or orderly fashion in accordance with this Directive; or

6.2.3. Follow directions of an Administrative Judge or the Appeal Board; then the Director, DOHA, or designee, may revoke any security clearance held by the applicant and discontinue case processing. Requests for resumption of case processing and reinstatement of a security clearance may be approved by the Director, DOHA, only upon a showing of good cause. If the request is denied, in whole or in part, the decision is final and bars reapplication for a security clearance for 1 year from the date of the revocation.

6.3. Each clearance decision must be a fair and impartial common sense determination based upon consideration of all the relevant and material information and the pertinent criteria and adjudication policy in enclosure 2, including as appropriate:

6.3.1. Nature and seriousness of the conduct and surrounding circumstances.

6.3.2. Frequency and recency of the conduct.

6.3.3. Age of the applicant.

6.3.4. Motivation of the applicant, and the extent to which the conduct was negligent, willful, voluntary, or undertaken with knowledge of the consequences involved.

6.3.5. Absence or presence of rehabilitation.

6.3.6. Probability that the circumstances or conduct will continue or recur in the future;

6.4. Whenever there is a reasonable basis for concluding that an applicant's continued access to classified information poses an imminent threat to the national interest, any security clearance held by the applicant may be suspended by the ASD(C3I), with the concurrence of the GC, DoD, pending a final clearance decision. This suspension may be rescinded by the same authorities upon presentation of additional information that conclusively demonstrates that an imminent threat to the national interest no longer exists. Procedures in enclosure 3 shall be expedited whenever an applicant's security clearance has been suspended pursuant to this subsection.

6.5. Nothing contained in this Directive shall limit or affect the responsibility and powers of the Secretary of Defense or the head of another Department or Agency to deny or revoke a security clearance when the security of the nation so requires. Such authority may not be delegated and may be exercised only when the Secretary of Defense or the head of another Department or Agency determines that the hearing procedures and other provisions of this Directive cannot be invoked consistent with the national security. Such a determination shall be conclusive.

6.6. Additional procedural guidance is in enclosure 3.

7. EFFECTIVE DATE

This Directive is effective March 16, 1992, except those cases in which a statement of reasons has been issued shall be concluded in accordance with DoD Directive 5220.6 (reference (a)).

Donald J. Atwood
Deputy Secretary of Defense

Enclosures -3

E1. Executive Order 10865, "Safeguarding Classified Information Within Industry," as amended by Executive Order No. 10909 of January 17, 1961, Executive Order No. 11382 of November 28, 1967, and Executive Order No. 12829 of January 6, 1993"

E2. Paragraph 2-200 and Appendix I, DoD 5200.2-R

E3. Additional Procedural Guidance

E1. ENCLOSURE 1

EXECUTIVE ORDER 10865*
SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY

Source: The provisions of Executive Order 10865 of Feb. 20, 1960, appear at 25 FR 1583, 3 CFR 1959-1963 Comp., p. 398, unless otherwise noted.

WHEREAS it is mandatory that the United States protect itself against hostile or destructive activities by preventing unauthorized disclosure of classified information relating to the national defense; and

WHEREAS it is a fundamental principle of our Government to protect the interests of individuals against unreasonable or unwarranted encroachment; and

WHEREAS I find that the provisions and procedures prescribed by this order are necessary to assure the preservation of the integrity of classified defense information and to protect the national interest; and

WHEREAS I find that those provisions and procedures recognize the interests of individuals affected thereby and provide maximum possible safeguards to protect such interest:

NOW, THEREFORE, under and by virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States and as Commander in Chief of the Armed Forces of the United States, it is hereby ordered as follows:

*Executive Order 10865, signed by President Eisenhower on Feb. 20, 1960, is hereby reprinted as amended by Executive Order No. 10909 of January 17, 1961, Executive Order No. 11382 of November 28, 1967, and Executive Order No. 12829 of January 6, 1993. This is an editorial format prepared by the Directorate for Industrial Security Clearance Review as one convenient source for subsequent changes to Executive Order 10865 and is not intended to be used as a definitive legal authority. This version incorporates amendments through January 6, 1993, by Presidents Dwight D. Eisenhower, Lyndon B. Johnson and George Bush.

SECTION 1. When used in this order, the term "head of a Department" means the Secretary of State, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, the Nuclear Regulatory Commission, the Administrator of the National Aeronautics and Space Administration, and, in section 4, the Attorney General. The term "head of a Department" also means the head of any Department or Agency, including but not limited to those referenced above with whom the Department of Defense makes an agreement to extend regulations prescribed by the Secretary of Defense concerning authorizations for access to classified information pursuant to Executive Order No. 12829.

[Sec. 1 amended by EO 10909 of Jan 17, 1961, 26 FR 508, 3 CFR, 1959-1963 Comp., p. 437; EO 11382 of Nov. 28, 1967, 32 FR 16247, 3 CFR, 1966-1970 Comp., p. 691; EO 12829 of Jan. 6, 1993, 58 FR 3479]

SECTION 2. An authorization for access to classified information pursuant to Executive Order No. 12829 may be granted by the head of a Department or his designee, including, but not limited to, those officials named in section 8 of this order, to an individual, hereinafter termed an "applicant", for a specific classification category only upon a finding that it is clearly consistent with the national interest to do so.

[Sec. 2 amended by EO 12829 of Jan 6, 1993, 58 F4 3479]

SECTION 3. Except as provided in section 9 of this order, an authorization for access to a specific classification category may not be finally denied or revoked pursuant to Executive Order 12829 by the head of a Department or his designee, including, but not limited to, those officials named in section 8 of this order, unless the applicant has been given the following:

(1) A written statement of reasons why his access authorization may be denied or revoked, which shall be as comprehensive and detailed as the national security permits.

(2) A reasonable opportunity to reply in writing under oath or affirmation to the statement of reasons.

(3) After he has filed under oath or affirmation a written reply to the statement of reasons, the form and sufficiency of which may be prescribed by regulations issued by the head of the Department concerned, an opportunity to appear personally before the head of the Department concerned or his designee, including, but not limited to, those

officials named in section 8 of this order, for the purpose of supporting his eligibility for access authorization and to present evidence on his behalf.

(4) A reasonable time to prepare for that appearance.

(5) An opportunity to be represented by counsel.

(6) An opportunity to cross-examine persons either orally or through written interrogatories in accordance with section 4 on matters not relating to the characterization in the statement of reasons of any organization or individual other than the applicant.

(7) A written notice of the final decision in his case which, if adverse, shall specify whether the head of the Department or his designee, including, but not limited to, those officials named in section 8 of this order, found for or against him with respect to each allegation in the statement of reasons.

[Sec. 3 amended by EO 12829 of Jan 6, 1993, 58 FR 3479]

SECTION 4. (a) An applicant shall be afforded an opportunity to cross-examine persons who have made oral or written statements adverse to the applicant relating to a controverted issue except that any such statement may be received and considered without affording such opportunity in the circumstances described in either of the following paragraphs:

(1) The head of the Department supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his identity would be substantially harmful to the national interest.

(2) The head of the Department concerned or his special designee for that particular purpose has preliminarily determined, after considering information furnished by the investigative agency involved as to the reliability of the person and the accuracy of the statement concerned, that the statement concerned appears to be reliable and material, and the head of the Department or such special designee has determined that failure to receive and consider such statement would, in view of the level of access sought, be substantially harmful to the national security and that the person who furnished the information cannot appear to testify (A) due to death, severe illness, or similar cause, in which case the identity of the person and the information to

be considered shall be made available to the applicant, or (B) due to some other cause determined by the head of the Department to be good and sufficient.

(b) Whenever procedures under paragraph (1) or (2) of subsection (a) of this section are used (1) the applicant shall be given a summary of the information which shall be as comprehensive and detailed as the national security permits, (2) appropriate consideration shall be accorded to the fact that the applicant did not have an opportunity to cross-examine such person or persons, and (3) a final determination adverse to the applicant shall be made only by the head of the Department based upon his personal review of the case.

SECTION 5. (a) Records compiled in the regular course of business, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that such information has been furnished to the Department concerned by an investigative agency pursuant to its responsibilities in connection with assisting the head of the Department concerned to safeguard classified information within industry pursuant to this order.

(b) Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue which, because they are classified, may not be inspected by the applicant, may be received and considered provided that: (1) the head of the Department concerned or his special designee for that purpose has made a preliminary determination that such physical evidence appears to be material, (2) the head of the Department concerned or such designee has made a determination that failure to receive and consider such physical evidence would, in view of the level of access sought, be substantially harmful to the national security, and (3) to the extent that the national security permits, a summary or description of such physical evidence is made available to the applicant. In every such case, information as to the authenticity and accuracy of such physical evidence furnished by the investigative agency involved shall be considered. In such instances a final determination adverse to the applicant shall be made only by the head of the Department based upon his personal review of the case.

SECTION 6. The head of a Department of the United States or his representative, may issue, in appropriate cases, invitations and requests to appear and testify in order that the applicant may have the opportunity to cross-examine as provided by this order. Whenever a witness is so invited or requested to appear and testify at a proceeding and the witness is an officer or employee of the Executive Branch of the Government or a member of the Armed Forces of the United States, and the proceeding involves the activity in connection with which the witness is employed,

travel expenses and per diem are authorized as provided by the Standard Government Travel Regulations or the Joint Travel Regulations, as appropriate. In all other cases (including non-Government employees as well as officers or employees of the Executive Branch of the Government or members of the Armed Forces of the United states not covered by the foregoing sentence), transportation in kind and reimbursement for actual expenses are authorized in an amount not to exceed the amount payable under Standardized Government Travel Regulations. An Officer or employee of the Executive Branch of the Government or a member of the Armed Forces of the United States who is invited or requested to appear pursuant to this paragraph shall be deemed to be in the performance of his official duties. So far as the national security permits, the head of the investigative agency involved shall cooperate with the Secretary, the Administrator, or the head of the other Department or Agency, as the case may be, in identifying persons who have made statements adverse to the applicant and in assisting him in making them available for cross-examination. If a person so invited is an officer or employee of the Executive Branch of the Government or a member of the Armed Forces of the United States, the head of the Department or Agency concerned shall cooperate in making that person available for cross-examination.

[Sec. 6 amended by EO 10909 of Jan. 17, 1961, 26 FR 508, 3 CFR, 1959-1963 Comp., p. 437; EO 11382 of Nov. 28, 1967, 32 FR 16247, 3 CFR, 1966-1970 Comp., p. 691; EO 12829 of Jan. 6, 1993, 58 FR 3479]

SECTION 7. Any determination under this order adverse to an applicant shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.

SECTION 8. Except as otherwise specified in the preceding provisions of this order, any authority vested in the head of a Department by this order may be delegated to the deputy of that Department, or the principal assistant to the head of that Department, as the case may be.

[Sec. 8 amended by EO 10909 of Jan 17, 1961, 26 FR 508, 3 CFR, 1959-1963 Comp., p. 437; EO 11382 of Nov. 28, 1967, 32 FR 16247, 3 CFR, 1966-1970 Comp., p. 691; EO 12829 of Jan. 6, 1993, 58 FR 3479]

SECTION 9. Nothing contained in this order shall be deemed to limit or affect the responsibility and powers of the head of a Department to deny or revoke access to a specific classification category if the security of the nation so requires. Such authority may not be delegated and may be exercised only when the head of a

Department determines that the procedures prescribed in sections 3, 4, and 5 cannot be invoked consistently with the national security and such determination shall be conclusive.

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

AUG 30 2006

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

Subject: Implementation of Adjudicative Guidelines for Determining Eligibility For Access to Classified Information (December 29, 2005)

This memorandum directs the implementation of the attached revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (December 29, 2005), as modified, effective September 1, 2006.

The revised Guidelines supersede the memorandum issued by the former Assistant Secretary of Defense for Command, Control, Communications, and Intelligence dated August 16, 2000, Subject: Guidance to DoD Central Adjudication Facilities (CAF) Clarifying the Application of the Foreign Preference Adjudicative Guideline.

The attachment incorporates the provisions of the "Smith Amendment," Section 986 of Title 10 of the United States Code, as amended. The Smith Amendment provides authority to grant an exception to the prohibition concerning persons convicted of a crime, sentenced to a term exceeding one year, and incarcerated for not less than one year, or who have been discharged or dismissed from the Armed Forces under dishonorable conditions. An exception to the Smith Amendment for the persons described above is only authorized by a designated waiver authority in meritorious cases where mitigating factors exist that are consistent with the mitigating factors described in the attached Adjudicative Guidelines.

The waiver authority formerly held by the Secretary of Defense is now delegated to the Director, Washington Headquarters Services (WHS) or designee, for its employees and those entities serviced by WHS; the Director, Defense Intelligence Agency (DIA) or designee, for its employees and those entities serviced by DIA; the Director, National Security Agency (NSA) or designee, for its employees and those entities serviced by NSA; the Director, Defense Office of Hearings and Appeals (DOHA) or designee, for an officer or employee of a DoD contractor serviced by DOHA; and the Secretaries of the Military Departments or designee. Waiver authority may not be further delegated to a member of the Component Personnel Security Appeal Board or the DOHA Security Clearance Appeal Board.

The revised Guidelines apply to all adjudications and other determinations made under the Department of Defense Directive (DoDD) 5220.6, January 2, 1992, Defense Industrial Personnel Security Clearance Review Program, and the DoD Personnel Security Program, DoD 5200.2-R, January 1, 1987. They replace the present guidelines published in Enclosure Two to DoDD 5220.6 and Appendix Eight to DoD 5200.2-R. Military Department and Defense Agency regulations should be revised in accordance with this memorandum.

The revised Guidelines apply to all adjudications and other determinations in which a Statement of Reasons has not been issued by September 1, 2006. All adjudications and other determinations in which a Statement of Reasons has been issued prior to September 1, 2006 will be made under the current Guidelines.

Stephen A. Cambone

Attachment:
As stated

Adjudicative Guidelines for Determining Eligibility For Access to Classified Information

1. *Introduction.* The following adjudicative guidelines are established for all U.S. 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. Government departments and agencies may also choose to apply these guidelines to analogous situations regarding persons being considered for access to other types of protected information.

Decisions regarding eligibility for access to classified information take into account factors that could cause a conflict of interest and place a person in the position of having to choose between his or her commitments to the United States, including the commitment to protect classified information, and any other compelling loyalty. Access decisions also take into account a person's reliability, trustworthiness and ability to protect classified information. No coercive policing could replace the self-discipline and integrity of the person entrusted with the nation's secrets as the most effective means of protecting them. When a person's life history shows evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on and trusted to exercise the responsibility necessary for working in a secure environment where protecting classified information is paramount.

2. *The 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 an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication 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 factors:

(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 extent to which participation is voluntary;

(6) the presence or absence of rehabilitation and other permanent behavioral changes;

(7) the motivation for the conduct;

(8) the potential for pressure, coercion, exploitation, or duress; and

(9) the likelihood of continuation or 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 concerning personnel being considered for access to classified information will be resolved in favor of the national security.

(c) The ability to develop specific thresholds for action under these guidelines is limited by the nature and complexity of human behavior. 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 judgment based upon careful consideration of the following guidelines, each of which is to be evaluated in the context of the whole person.

(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: Psychological Conditions;

(10) GUIDELINE J: Criminal Conduct;

(11) GUIDELINE K: Handling Protected Information;

(12) GUIDELINE L: Outside Activities;

(13) GUIDELINE M: Use 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 investigation 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.

GUIDELINE A: ALLEGIANCE TO THE UNITED STATES

3. *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.

4. *Conditions that could raise a security concern and may be disqualifying include:*

(a) involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the United States of America;

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

(c) association or sympathy with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means, in an effort to:

(1) overthrow or influence the government of the United States or any state or local government;

(2) prevent Federal, state, or local government personnel from performing their official duties;

(3) gain retribution for perceived wrongs caused by the Federal, state, or local government;

(4) prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

5. *Conditions that could mitigate security concerns include:*

(a) the individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

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

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

(d) the involvement or association with such activities occurred under such unusual circumstances, or so much time has elapsed, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or loyalty.

GUIDELINE B: FOREIGN INFLUENCE

6. *The Concern.* Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercion by any foreign interest. Adjudication under this Guideline can and should consider the identity of the foreign country in which the foreign contact or financial interest is located, including, but not limited to, such considerations as whether the foreign country is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism.

7. *Conditions that could raise a security concern and may be disqualifying include:*

(a) contact with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion;

(b) connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information;

(c) counterintelligence information, that may be classified, indicates that the individual's access to protected information may involve unacceptable risk to national security;

(d) sharing living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion;

(e) a substantial business, financial, or property interest in a foreign country, or in any foreign-owned or foreign-operated business, which could subject the individual to heightened risk of foreign influence or exploitation;

(f) failure to report, when required, association with a foreign national;

(g) unauthorized association with a suspected or known agent, associate, or employee of a foreign intelligence service;

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

(i) conduct, especially while traveling outside the U.S., which may make the individual vulnerable to exploitation, pressure, or coercion by a foreign person, group, government, or country.

8. *Conditions that could mitigate security concerns include:*

(a) the nature of the relationships with foreign persons, the country in which these persons are located, or the positions or activities of those persons in that country are such that it is unlikely the individual will be placed in a position of having to choose between the interests of a foreign individual, group, organization, or government and the interests of the U.S.;

(b) there is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the U.S., that the individual can be expected to resolve any conflict of interest in favor of the U.S. interest;

(c) contact or communication with foreign citizens is so casual and infrequent that there is little likelihood that it could create a risk for foreign influence or exploitation;

(d) the foreign contacts and activities are on U.S. Government business or are approved by the cognizant security authority;

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

(f) the value or routine nature of the foreign business, financial, or property interests is such that they are unlikely to result in a conflict and could not be used effectively to influence, manipulate, or pressure the individual.

GUIDELINE C: FOREIGN PREFERENCE

9. *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.

10. *Conditions that could raise a security concern and may be disqualifying include:*

(a) exercise of any right, privilege or obligation of foreign citizenship after becoming a U.S. citizen or through the foreign citizenship of a family member. This includes but is not limited to:

(1) possession of a current foreign passport;

(2) military service or a willingness to bear arms for a foreign country;

(3) accepting educational, medical, retirement, social welfare, or other such benefits from a foreign country;

(4) residence in a foreign country to meet citizenship requirements;

(5) using foreign citizenship to protect financial or business interests in another country;

(6) seeking or holding political office in a foreign country;

(7) voting in a foreign election;

(b) action to acquire or obtain recognition of a foreign citizenship by an American citizen;

(c) performing or attempting to perform duties, or otherwise acting, so as to serve the interests of a foreign person, group, organization, or government in conflict with the national security interest;

(d) any statement or action that shows allegiance to a country other than the United States: for example, declaration of intent to renounce United States citizenship; renunciation of United States citizenship.

11. *Conditions that could mitigate security concerns include:*

(a) dual citizenship is based solely on parents' citizenship or birth in a foreign country;

(b) the individual has expressed a willingness to renounce dual citizenship;

(c) exercise of the rights, privileges, or obligations of foreign citizenship occurred before the individual became a U.S. citizen or when the individual was a minor;

(d) use of a foreign passport is approved by the cognizant security authority.

(e) the passport has been destroyed, surrendered to the cognizant security authority, or otherwise invalidated;

(f) the vote in a foreign election was encouraged by the United States Government.

GUIDELINE D: SEXUAL BEHAVIOR

12. *The Concern.* Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. No adverse inference concerning the standards in this Guideline may be raised solely on the basis of the sexual orientation of the individual.

13. *Conditions that could raise a security concern and may be disqualifying include*:

(a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(b) a pattern of compulsive, self-destructive, or high risk sexual behavior that the person is unable to stop or that may be symptomatic of a personality disorder;

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

(d) sexual behavior of a public nature and/or that reflects lack of discretion or judgment.

14. *Conditions that could mitigate security concerns include*:

(a) the behavior occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature;

(b) the sexual behavior happened so long ago, so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

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

(d) the sexual behavior is strictly private, consensual, and discreet.

GUIDELINE E: PERSONAL CONDUCT

15. *The Concern.* Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, and cooperation with medical or psychological evaluation;

(b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

16. *Conditions that could raise a security concern and may be disqualifying include:*

(a) deliberate omission, concealment, or falsification of relevant 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;

(b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative;

(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information;

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but

which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information:

(2) disruptive, violent, or other inappropriate behavior in the workplace;

(3) a pattern of dishonesty or rule violations;

(4) evidence of significant misuse of Government or other employer's time or resources;

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group;

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment;

(g) association with persons involved in criminal activity.

17. *Conditions that could mitigate security concerns include:*

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully.

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;

(f) the information was unsubstantiated or from a source of questionable reliability;

(g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

GUIDELINE F: FINANCIAL CONSIDERATIONS

18. *The Concern.* Failure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Compulsive gambling is a concern as it may lead to financial crimes including espionage. Affluence that cannot be explained by known sources of income is also a security concern. It may indicate proceeds from financially profitable criminal acts.

19. *Conditions that could raise a security concern and may be disqualifying include:*

(a) inability or unwillingness to satisfy debts;

(b) indebtedness caused by frivolous or irresponsible spending and the absence of any evidence of willingness or intent to pay the debt or establish a realistic plan to pay the debt.

(c) a history of not meeting financial obligations;

(d) 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;

(e) consistent spending beyond one's means, which may be indicated by excessive indebtedness, significant negative cash flow, high debt-to-income ratio, and/or other financial analysis;

(f) financial problems that are linked to drug abuse, alcoholism, gambling problems, or other issues of security concern;

(g) failure to file annual Federal, state, or local income tax returns as required or the fraudulent filing of the same;

(h) unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that cannot be explained by subject's known legal sources of income;

(i) compulsive or addictive gambling as indicated by an unsuccessful attempt to stop gambling, "chasing losses" (i.e. increasing the bets or returning another day in an effort to get even), concealment of gambling losses, borrowing money to

fund gambling or pay gambling debts, family conflict or other problems caused by gambling.

20. *Conditions that could mitigate security concerns include*:

(a) the behavior happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the conditions that resulted in the financial problem were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation), and the individual acted responsibly under the circumstances;

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

(d) the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts;

(e) the individual has a reasonable basis to dispute the legitimacy of the past-due debt which is the cause of the problem and provides documented proof to substantiate the basis of the dispute or provides evidence of actions to resolve the issue;

(f) the affluence resulted from a legal source of income.

GUIDELINE G: ALCOHOL CONSUMPTION

21. *The Concern.* Excessive alcohol consumption often leads to the exercise of questionable judgment or the failure to control impulses, and can raise questions about an individual's reliability and trustworthiness.

22. *Conditions that could raise a security concern and may be disqualifying include:*

(a) alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, disturbing the peace, or other incidents of concern, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(b) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(c) habitual or binge consumption of alcohol to the point of impaired judgment, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(d) diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

(e) evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

(f) relapse after diagnosis of alcohol abuse or dependence and completion of an alcohol rehabilitation program;

(g) failure to follow any court order regarding alcohol education, evaluation, treatment, or abstinence.

23. *Conditions that could mitigate security concerns include:*

(a) so much time has passed, or the behavior was so infrequent, or it happened under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the individual acknowledges his or her alcoholism or issues of alcohol abuse, provides evidence of actions taken to overcome this problem, and has established a pattern of abstinence (if alcohol dependent) or responsible use (if an alcohol abuser);

(c) the individual is a current employee who is participating in a counseling or treatment program, has no history of previous treatment and relapse, and is making satisfactory progress;

(d) the individual has successfully completed inpatient or outpatient counseling or rehabilitation along with any required aftercare, has demonstrated a clear and established pattern of modified consumption or abstinence in accordance with treatment recommendations, such as participation in meetings of Alcoholics Anonymous or a similar organization and has received a favorable prognosis by a duly qualified medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

GUIDELINE H: DRUG INVOLVEMENT

24. *The Concern.* Use of an illegal drug or misuse of a prescription drug can raise questions about an individual's reliability and trustworthiness, both because it may impair judgment and because it raises questions about a person's ability or willingness to comply with laws, rules, and regulations.

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

(1) 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), and

(2) inhalants and other similar substances;

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

25. *Conditions that could raise a security concern and may be disqualifying include*:

(a) any drug abuse (see above definition);[1]

(b) testing positive for illegal drug use;

(c) illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia;

(d) diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

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

(f) failure to successfully complete a drug treatment program prescribed by a duly qualified medical professional;

(g) any illegal drug use after being granted a security clearance;

(h) expressed intent to continue illegal drug use, or failure to clearly and convincingly commit to discontinue drug use.

26. *Conditions that could mitigate security concerns include*:

1 Under the provisions of 10 U.S.C. 986 any person who is an unlawful user of, or is addicted to, a controlled substance as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802), may not be granted or have renewed their access to classified information.

(a) the behavior happened so long ago, was so infrequent, or happened under such circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) a demonstrated intent not to abuse any drugs in the future, such as:

(1) disassociation from drug-using associates and contacts;

(2) changing or avoiding the environment where drugs were used;

(3) an appropriate period of abstinence;

(4) a signed statement of intent with automatic revocation of clearance for any violation;

(c) abuse of prescription drugs was after a severe or prolonged illness during which these drugs were prescribed, and abuse has since ended;

(d) satisfactory completion of a prescribed drug treatment program, including but not limited to rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a duly qualified medical professional.

GUIDELINE I: PSYCHOLOGICAL CONDITIONS

27. *The Concern.* Certain emotional, mental, and personality conditions can impair judgment, reliability, or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline. A duly qualified mental health professional (e.g., clinical psychologist or psychiatrist) employed by, or acceptable to and approved by the U.S. Government, should be consulted when evaluating potentially disqualifying and mitigating information under this guideline. No negative inference concerning the standards in this Guideline may be raised solely on the basis of seeking mental health counseling.

28. *Conditions that could raise a security concern and may be disqualifying include:*

(a) behavior that casts doubt on an individual's judgment, reliability, or trustworthiness that is not covered under any other guideline, including but not limited to emotionally unstable, irresponsible, dysfunctional, violent, paranoid, or bizarre behavior;

(b) an opinion by a duly qualified mental health professional that the individual has a condition not covered under any other guideline that may impair judgment, reliability, or trustworthiness;[1]

(c) the individual has failed to follow treatment advice related to a diagnosed emotional, mental, or personality condition, e.g., failure to take prescribed medication.

29. *Conditions that could mitigate security concerns include:*

(a) the identified condition is readily controllable with treatment, and the individual has demonstrated ongoing and consistent compliance with the treatment plan;

(b) the individual has voluntarily entered a counseling or treatment program for a condition that is amenable to treatment, and the individual is currently receiving counseling or treatment with a favorable prognosis by a duly qualified mental health professional;

(c) recent opinion by a duly qualified mental health professional employed by, or acceptable to and approved by the U.S. Government that an individual's

1 Under the provisions of 10 U.S.C. 986, and person who is mentally incompetent, as determined by a credentialed mental health professional approved by the Department of Defense, may not be granted or have renewed their access to classified information.

previous condition is under control or in remission, and has a low probability of recurrence or exacerbation;

(d) the past emotional instability was a temporary condition (e.g., one caused by death, illness, or marital breakup), the situation has been resolved, and the individual no longer shows indications of emotional instability;

(e) there is no indication of a current problem.

GUIDELINE J: CRIMINAL CONDUCT

30. *The Concern.* Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

31. *Conditions that could raise a security concern and may be disqualifying include*:

(a) a single serious crime or multiple lesser offenses;

(b) discharge or dismissal from the Armed Forces under dishonorable conditions;[1]

(c) allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted;

(d) individual is currently on parole or probation;

(e) violation of parole or probation, or failure to complete a court-mandated rehabilitation program;

(f) *conviction in a Federal or State court, including a court-martial of a crime, sentenced to imprisonment for a term exceeding one year and incarcerated as a result of that sentence for not less than a year.*[2]

32. *Conditions that could mitigate security concerns include*:

(a) so much time has elapsed since the criminal behavior happened, or it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

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

(c) evidence that the person did not commit the offense;

---

1 Under the provisions of 10 U.S.C. 986, a person who has received a dishonorable discharge or has been dismissed from the Armed Forces may not be granted or have renewed access to classified information. In a meritorious case, the Secretaries of the Military Departments or designee, or the Directors of WHS, DIA, NSA, DOHA or designee may authorize a waiver of this prohibition. Waiver authority may not be further delegated to a member of the Component Personnel Security Appeal Board or the DOHA Security Clearance Appeal Board.

2 Under the above mentioned statute, a person who has been convicted in a Federal or State court, including courts martial, sentenced to imprisonment for a term exceeding one year and incarcerated for not less than one year, may not be granted or have renewed access to classified information. The same waiver provision also applies.

(d) there is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community involvement;

(e) *potentially disqualifying conditions (b) and (f) above, may not be mitigated unless, where meritorious circumstances exist, the Secretaries of the Military Departments or designee; or the Directors of Washington Headquarters Services (WHS), Defense Intelligence Agency (DIA), National Security Agency (NSA), Defense Office of Hearings and Appeals (DOHA) or designee, has granted a waiver.*

GUIDELINE K: HANDLING PROTECTED INFORMATION

33. *The Concern.* Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

34. *Conditions that could raise a security concern and may be disqualifying include*:

(a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;

(b) collecting or storing classified or other protected information at home or in any other unauthorized location;

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;

(d) inappropriate efforts to obtain or view classified or other protected information outside one's need to know;

(e) copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings;

(f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;

(g) any failure to comply with rules for the protection of classified or other sensitive information;

(h) negligence or lax security habits that persist despite counseling by management.

(i) failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent.

35. *Conditions that could mitigate security concerns include*:

(a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and

does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;

(c) the security violations were due to improper or inadequate training.

GUIDELINE L: OUTSIDE ACTIVITIES

36. *The Concern.* Involvement in certain types of outside employment or activities is of security concern if it poses a conflict of interest with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

37. *Conditions that could raise a security concern and may be disqualifying include:*

(a) any employment or service, whether compensated or volunteer, with:

(1) the government of a foreign country;

(2) any foreign national, organization, or other entity;

(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;

(b) failure to report or fully disclose an outside activity when this is required.

38. *Conditions that could mitigate security concerns include:*

(a) evaluation of the outside employment or activity by the appropriate security or counterintelligence office indicates that it does not pose a conflict with an individual's security responsibilities or with the national security interests of the United States;

(b) the individual terminated the employment or discontinued the activity upon being notified that it was in conflict with his or her security responsibilities.

GUIDELINE M: USE OF INFORMATION TECHNOLOGY SYSTEMS

39. *The Concern.* Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

40. *Conditions that could raise a security concern and may be disqualifying include:*

(a) illegal or unauthorized entry into any information technology system or component thereof;

(b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

(e) unauthorized use of a government or other information technology system;

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations;

(g) negligence or lax security habits in handling information technology that persist despite counseling by management;

(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

41. *Conditions that could mitigate security concerns include:*

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available;

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

E3. ENCLOSURE 3

ADDITIONAL PROCEDURAL GUIDANCE

E3.1.1. When the DISCO cannot affirmatively find that it is clearly consistent with the national interest to grant or continue a security clearance for an applicant, the case shall be promptly referred to the DOHA.

E3.1.2. Upon referral, the DOHA shall make a prompt determination whether to grant or continue a security clearance, issue a statement of reasons (SOR) as to why it is not clearly consistent with the national interest to do so, or take interim actions, including but not limited to:

E3.1.2.1. Direct further investigation.

E3.1.2.2. Propound written interrogatories to the applicant or other persons with relevant information.

E3.1.2.3. Requiring the applicant to undergo a medical evaluation by a DoD Psychiatric Consultant.

E3.1.2.4. Interviewing the applicant.

E3.1.3. An unfavorable clearance decision shall not be made unless the applicant has been provided with a written SOR that shall be as detailed and comprehensive as the national security permits. A letter of instruction with the SOR shall explain that the applicant or Department Counsel may request a hearing. It shall also explain the adverse consequences for failure to respond to the SOR within the prescribed time frame.

E3.1.4. The applicant must submit a detailed written answer to the SOR under oath or affirmation that shall admit or deny each listed allegation. A general denial or other similar answer is insufficient. To be entitled to a hearing, the applicant must specifically request a hearing in his or her answer. The answer must be received by the DOHA within 20 days from receipt of the SOR. Requests for an extension of time to file an answer may be submitted to the Director, DOHA, or designee, who in turn may grant the extension only upon a showing of good cause.

E3.1.5. If the applicant does not file a timely and responsive answer to the SOR, the Director, DOHA, or designee, may discontinue processing the case, deny issuance

of the requested security clearance, and direct the DISCO to revoke any security clearance held by the applicant.

E3.1.6. Should review of the applicant's answer to the SOR indicate that allegations are unfounded, or evidence is insufficient for further processing, Department Counsel shall take such action as appropriate under the circumstances, including but not limited to withdrawal of the SOR and transmittal to the Director for notification of the DISCO for appropriate action.

E3.1.7. If the applicant has not requested a hearing with his or her answer to the SOR and Department Counsel has not requested a hearing within 20 days of receipt of the applicant's answer, the case shall be assigned to the Administrative Judge for a clearance decision based on the written record. Department Counsel shall provide the applicant with a copy of all relevant and material information that could be adduced at a hearing. The applicant shall have 30 days from receipt of the information in which to submit a documentary response setting forth objections, rebuttal, extenuation, mitigation, or explanation, as appropriate.

E3.1.8. If a hearing is requested by the applicant or Department Counsel, the case shall be assigned to the Administrative Judge for a clearance decision based on the hearing record. Following issuance of a notice of hearing by the Administrative Judge, or designee, the applicant shall appear in person with or without counsel or a personal representative at a time and place designated by the notice of hearing. The applicant shall have a reasonable amount of time to prepare his or her case. The applicant shall be notified at least 15 days in advance of the time and place of the hearing, which generally shall be held at a location in the United States within a metropolitan area near the applicant's place of employment or residence. A continuance may be granted by the Administrative Judge only for good cause. Hearings may be held outside of the United States in NATO cases, or in other cases upon a finding of good cause by the Director, DOHA, or designee.

E3.1.9. The Administrative Judge may require a pre-hearing conference.

E3.1.10. The Administrative Judge may rule on questions on procedure, discovery, and evidence and shall conduct all proceedings in a fair, timely, and orderly manner.

E3.1.11. Discovery by the applicant is limited to non-privileged documents and materials subject to control by the DOHA. Discovery by Department Counsel after

issuance of an SOR may be granted by the Administrative Judge only upon a showing of good cause.

E3.1.12. A hearing shall be open except when the applicant requests that it be closed, or when the Administrative Judge determines that there is a need to protect classified information or there is other good cause for keeping the proceeding closed. No inference shall be drawn as to the merits of a case on the basis of a request that the hearing be closed.

E3.1.13. As far in advance as practical, Department Counsel and the applicant shall serve one another with a copy of any pleading, proposed documentary evidence, or other written communication to be submitted to the Administrative Judge.

E3.1.14. Department Counsel is responsible for presenting witnesses and other evidence to establish facts alleged in the SOR that have been controverted.

E3.1.15. The applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision.

E3.1.16. Witnesses shall be subject to cross-examination.

E3.1.17. The SOR may be amended at the hearing by the Administrative Judge on his or her own motion, or upon motion by Department Counsel or the applicant, so as to render it in conformity with the evidence admitted or for other good cause. When such amendments are made, the Administrative Judge may grant either party's request for such additional time as the Administrative Judge may deem appropriate for further preparation or other good cause.

E3.1.18. The Administrative Judge hearing the case shall notify the applicant and all witnesses testifying that 18 U.S. C. 1001 (reference (c)) is applicable.

E3.1.19. The Federal Rules of Evidence (28 U.S. C. 101 et seq. (reference (d)) shall serve as a guide. Relevant and material evidence may be received subject to rebuttal, and technical rules of evidence may be relaxed, except as otherwise provided herein, to permit the development of a full and complete record.

E3.1.20. Official records or evidence compiled or created in the regular course of business, other than DoD personnel background reports of investigation (ROI), may be received and considered by the Administrative Judge without authenticating witnesses,

provided that such information has been furnished by an investigative agency pursuant to its responsibilities in connection with assisting the Secretary of Defense, or the Department or Agency head concerned, to safeguard classified information within industry under E.O. 10865 (enclosure 1.). An ROI may be received with an authenticating witness provided it is otherwise admissible under the Federal Rules of Evidence (28 U.S. C. 101 et seq. (reference (d)).

E3.1.21. Records that cannot be inspected by the applicant because they are classified may be received and considered by the Administrative Judge, provided the GC, DoD, has:

E3.1.21.1. Made a preliminary determination that such evidence appears to be relevant and material.

E3.1.21.2. Determined that failure to receive and consider such evidence would be substantially harmful to the national security.

E3.1.22. A written or oral statement adverse to the applicant on a controverted issue may be received and considered by the Administrative Judge without affording an opportunity to cross-examine the person making the statement orally, or in writing when justified by the circumstances, only in either of the following circumstances:

E3.1.22.1. If the head of the Department or Agency supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his or her identity would be substantially harmful to the national interest; or

E3.1.22.2. If the GC, DoD, has determined the statement concerned appears to be relevant, material, and reliable; failure to receive and consider the statement would be substantially harmful to the national security; and the person who furnished the information cannot appear to testify due to the following:

E3.1.22.2.1. Death, severe illness, or similar cause, in which case the identity of the person and the information to be considered shall be made available to the applicant; or

E3.1.22.2.2. Some other cause determined by the Secretary of Defense, or when appropriate by the Department or Agency head, to be good and sufficient.

E3.1.23. Whenever evidence is received under items E3.1.21. or E3.1.22., above,

the applicant shall be furnished with as comprehensive and detailed a summary of the information as the national security permits. The Administrative Judge and Appeal Board may make a clearance decision either favorable or unfavorable to the applicant based on such evidence after giving appropriate consideration to the fact that the applicant did not have an opportunity to confront such evidence, but any final determination adverse to the applicant shall be made only by the Secretary of Defense, or the Department or Agency head, based on a personal review of the case record.

E3.1.24. A verbatim transcript shall be made of the hearing. The applicant shall be furnished one copy of the transcript, less the exhibits, without cost.

E3.1.25. The Administrative Judge shall make a written clearance decision in a timely manner setting forth pertinent findings of fact, policies, and conclusions as to the allegations in the SOR, and whether it is clearly consistent with the national interest to grant or continue a security clearance for the applicant. The applicant and Department Counsel shall each be provided a copy of the clearance decision. In cases in which evidence is received under items E3.1.21. and E3.1.22., above, the Administrative Judge's written clearance decision may require deletions in the interest of national security.

E3.1.26. If the Administrative Judge decides that it is clearly consistent with the national interest for the applicant to be granted or to retain a security clearance, the DISCO shall be so notified by the Director, DOHA, or designee, when the clearance decision becomes final in accordance with item E3.1.36., below.

E3.1.27. If the Administrative Judge decides that it is not clearly consistent with the national interest for the applicant to be granted or to retain a security clearance, the Director, DOHA, or designee, shall expeditiously notify the DISCO, which shall in turn notify the applicant's employer of the denial or revocation of the applicant's security clearance. The letter forwarding the Administrative Judge's clearance decision to the applicant shall advise the applicant that these actions are being taken, and that the applicant may appeal the Administrative Judge's clearance decision.

E3.1.28. The applicant or Department Counsel may appeal the Administrative Judge's clearance decision by filing a written notice of appeal with the Appeal Board within 15 days after the date of the Administrative Judge's clearance decision. A notice of appeal received after 15 days from the date of the clearance decision shall not be accepted by the Appeal Board, or designated Board Member, except for good cause. A notice of cross-appeal may be filed with the Appeal Board within 10 days of receipt of the notice of appeal. An untimely cross appeal shall not be accepted by the

Appeal Board, or designated Board Member, except for good cause.

E3.1.29. Upon receipt of a notice of appeal, the Appeal Board shall be provided the case record. No new evidence shall be received or considered by the Appeal Board.

E3.1.30. After filing a timely notice of appeal, a written appeal brief must be received by the Appeal Board within 45 days from the date of the Administrative Judge's clearance decision. The appeal brief must state the specific issue or issues being raised, and cite specific portions of the case record supporting any alleged error. A written reply brief, if any, must be filed within 20 days from receipt of the appeal brief. A copy of any brief filed must be served upon the applicant or Department Counsel, as appropriate.

E3.1.31. Requests for extension of time for submission of briefs may be submitted to the Appeal Board or designated Board Member. A copy of any request for extension of time must be served on the opposing party at the time of submission. The Appeal Board, or designated Board Member, shall be responsible for controlling the Appeal Board's docket, and may enter an order dismissing an appeal in an appropriate case or vacate such an order upon a showing of good cause.

E3.1.32. The Appeal Board shall address the material issues raised by the parties to determine whether harmful error occurred. Its scope of review shall be to determine whether or not:

E3.1.32.1. The Administrative Judge's findings of fact are supported by such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record. In making this review, the Appeal Board shall give deference to the credibility determinations of the Administrative Judge;

E3.1.32.2. The Administrative Judge adhered to the procedures required by E.O. 10865 (enclosure 1.) and this Directive; or

E3.1.32.3. The Administrative Judge's rulings or conclusions are arbitrary, capricious, or contrary to law.

E3.1.33. The Appeal Board shall issue a written clearance decision addressing the material issues raised on appeal. The Appeal Board shall have authority to:

E3.1.33.1. Affirm the decision of the Administrative Judge;

E3.1.33.2. Remand the case to an Administrative Judge to correct identified error. If the case is remanded, the Appeal Board shall specify the action to be taken on remand; or

E3.1.33.3. Reverse the decision of the Administrative Judge if correction of identified error mandates such action.

E3.1.34. A copy of the Appeal Board's written clearance decision shall be provided to the parties. In cases in which evidence was received under items E3.1.21. and E3.1.22., above, the Appeal Board's clearance decision may require deletions in the interest of national security.

E3.1.35. Upon remand, the case file shall be assigned to an Administrative Judge for correction of error(s) in accordance with the Appeal Board's clearance decision. The assigned Administrative Judge shall make a new clearance decision in the case after correcting the error(s) identified by the Appeal Board. The Administrative Judge's clearance decision after remand shall be provided to the parties. The clearance decision after remand may be appealed pursuant to items E3.1.28. to E3.1.35., above.

E3.1.36. A clearance decision shall be considered final when:

E3.1.36.1. A security clearance is granted or continued pursuant to item E3.1.2., above;

E3.1.36.2. No timely notice of appeal is filed;

E3.1.36.3. No timely appeal brief is filed after a notice of appeal has been filed;

E3.1.36.4. The appeal has been withdrawn;

E3.1.36.5. When the Appeal Board affirms or reverses an Administrative Judge's clearance decision; or

E3.1.36.6. When a decision has been made by the Secretary of Defense, or the Department or Agency head, under to item E3.1.23., above. The Director, DOHA, or designee, shall notify the DISCO of all final clearance decisions.

E3.1.37. An applicant whose security clearance has been finally denied or

revoked by the DOHA is barred from reapplication for 1 year from the date of the initial unfavorable clearance decision.

E3.1.38. A reapplication for a security clearance must be made initially by the applicant's employer to the DISCO and is subject to the same processing requirements as those for a new security clearance application. The applicant shall thereafter be advised he is responsible for providing the Director, DOHA, with a copy of any adverse clearance decision together with evidence that circumstances or conditions previously found against the applicant have been rectified or sufficiently mitigated to warrant reconsideration.

E3.1.39. If the Director, DOHA, determines that reconsideration is warranted, the case shall be subject to this Directive for making a clearance decision.

E3.1.40. If the Director, DOHA, determines that reconsideration is not warranted, the DOHA shall notify the applicant of this decision. Such a decision is final and bars further reapplication for an additional one year period from the date of the decision rejecting the reapplication.

E3.1.41. Nothing in this Directive is intended to give an applicant reapplying for a security clearance any greater rights than those applicable to any other applicant under this Directive.

E3.1.42. An applicant may file a written petition, under oath or affirmation, for reimbursement of loss of earnings resulting from the suspension, revocation, or denial of his or her security clearance. The petition for reimbursement must include as an attachment the favorable clearance decision and documentation supporting the reimbursement claim. The Director, DOHA, or designee, may in his or her discretion require additional information from the petitioner.

E3.1.43. Claims for reimbursement must be filed with the Director, DOHA, or designee, within 1 year after the date the security clearance is granted. Department Counsel generally shall file a response within 60 days after receipt of applicant's petition for reimbursement and provide a copy thereof to the applicant.

E3.1.44. Reimbursement is authorized only if the applicant demonstrates by clear and convincing evidence to the Director, DOHA, that all of the following conditions are met:

E3.1.44.1. The suspension, denial, or revocation was the primary cause of the claimed pecuniary loss; and

E3.1.44.2. The suspension, denial, or revocation was due to gross negligence of the Department of Defense at the time the action was taken, and not in any way by the applicant's failure or refusal to cooperate.

E3.1.45. The amount of reimbursement shall not exceed the difference between the earnings of the applicant at the time of the suspension, revocation, or denial and the applicant's interim earnings, and further shall be subject to reasonable efforts on the part of the applicant to mitigate any loss of earnings. No reimbursement shall be allowed for any period of undue delay resulting from the applicant's acts or failure to act. Reimbursement is not authorized for loss of merit raises and general increases, loss of employment opportunities, counsel's fees, or other costs relating to proceedings under this Directive.

E3.1.46. Claims approved by the Director, DOHA, shall be forwarded to the Department or Agency concerned for payment. Any payment made in response to a claim for reimbursement shall be in full satisfaction of any further claim against the United States or any Federal Department or Agency, or any of its officers or employees.

E3.1.47. Clearance decisions issued by Administrative Judges and the Appeal Board shall be indexed and made available in redacted form to the public.