

Pt. 147

(d) of this section, when deemed appropriate with the facts and circumstances of each particular case, following consultation with legal staff.

(b) If a DoD member is the subject of the request, the member shall be ordered, under 10 U.S.C. 814, to return expeditiously to an appropriate port of entry at Government expense, contingent on the party requesting return of the member providing for transportation, and escort, if desired, of the member from such port of entry to the jurisdiction of the party. The party requesting return of the member shall be notified at least 10 days before the member's return to the selected port of entry, absent unusual circumstances.

(c) If a DoD employee is the subject of the request concerning the court order, the employee strongly shall be encouraged to comply with the court order. Failure to respond to the court order may be a basis for withdrawal of command sponsorship and may be the basis for adverse action against the DoD employee, to include removal from the Federal Service. Proposals to take such adverse action must be approved by the Head of the DoD Component concerned, or designee. Such proposals shall be coordinated with the cognizant civilian personnel office and legal counsel.

(d) If the family member of a DoD member or employee is the subject of a request concerning the court order, the family member strongly shall be encouraged to comply with the court order. Failure to respond to the court order may be a basis for withdrawing the command sponsorship of the family member.

[54 FR 298, Jan. 5, 1989, as amended at 55 FR 34555, Aug. 23, 1990]

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.

32 CFR Ch. I (7–1–00 Edition)

- 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).

SOURCE: 63 FR 4573, Jan. 30, 1998, unless otherwise noted.

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.

§ 147.3

(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;

32 CFR Ch. I (7–1–00 Edition)

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

¹The adjudicator should also consider guidelines pertaining to criminal conduct (Guideline J) and emotional, mental and personality disorders (Guideline I) in determining how to resolve the security concerns raised by sexual behavior.

(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;

(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 engag-

ing 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.

§ 147.10 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

§ 147.11

32 CFR Ch. I (7–1–00 Edition)

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;

Office of the Secretary of Defense

§ 147.15

(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 regrating 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, co-workers, 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 NACL or SSBI.	NACL	A
Top Secret, SCI; "Q"	Conf, Sec; "L" None None; Conf, Sec; "L".	None Current or out of date NACL 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 month's or more
Confidential	0 to 14 years. 11 mos	None (note 1)	NACL
	15 yrs. or more	NACL.	
Secret; "L"	0 to 9 yrs 11 mos	None (note 1).	

TABLE 2.—REINVESTIGATION REQUIREMENTS—Continued

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
Top Secret, SCI; “Q”	10 yrs. or more 0 to 4 yrs. 11 mos 5 yrs or more	NACLCLC None (note 1) SSBI–PR.	SSBI

Note: As a minimum, review an updated Standard Form 84 and applicable records. A reinvestigation (NACLCLC 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 sub-

mission of a request for an expedited National Agency Check with Local Agency Checks and Credit (NACLCLC).

§ 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 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*.

PART 148—NATIONAL POLICY AND IMPLEMENTATION OF RECIPROCI- TY OF FACILITIES**Subpart A—National Policy on Reciprocity of Use and Inspections of Facilities**

Sec.

- 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.)

SOURCE: 63 FR 4580, Jan. 30, 1998, unless otherwise noted.

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

CARNEGIE MELLON ENGINEERING SCHOOL CERT INSIDER THREAT BEST PRACTICES:

Common Sense Guide	Best Practice
1	Know and protect your critical assets (e.g., what sensitive assets are accessible in the manager's role).
2	Develop a formalized documented insider threat program.
3	Clearly document and consistently enforce policies and controls.
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5	Anticipate and manage negative issues in the work environment.
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.
7	Be especially vigilant regarding social media.
8	Structure management and tasks to minimize unintentional insider stress and mistakes.
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.
10	Implement strict password and account management policies and practices.
11	Institute stringent access controls and monitoring policies on privileged users.
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
13	Monitor and control remote access from all end points, including mobile devices.
14	Establish a baseline of normal behavior for both networks and employees.
15	Enforce separation of duties and least privilege.
16	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
17	Institutionalize system change controls.

Common Sense Guide	Best Practice
18	Implement secure backup and recovery processes.
19	Close the doors to unauthorized data exfiltration.
20	Develop a comprehensive employee termination procedure.