

Click the "X" in the upper right corner to close this page.

Purpose



The DLA Personnel Security Program is designed to ensure that only loyal, trustworthy, and reliable people are assigned to sensitive duties or granted access to classified information.

Personnel security is an increasingly complex and expensive investment that is fundamental to the security of the nation. The federal government must maintain the very best personnel security systems for the safety of both the citizens we serve and those who have the honor of serving within our government.

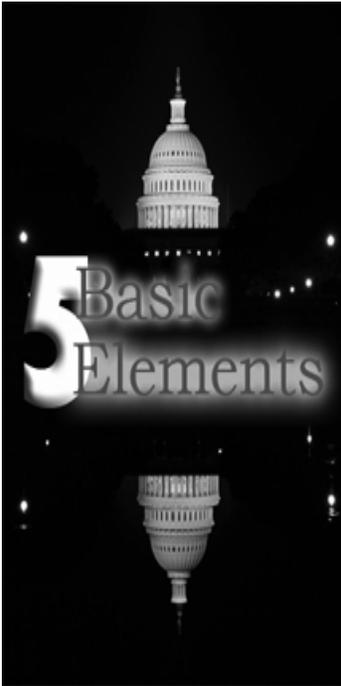
Source: "OPM Director Kay Coles James Emphasizes Importance of Personnel Security to the Nation," U.S. Office of Personnel Management news release, January 30, 2004.

Note:

Kay Coles James served as the Director of the Office of Personnel Management (OPM) from 2001 to 2005

Lesson Content

Five Basic Elements



The Personnel Security Program consists of five basic elements. We will address each one in this section. The following are the five elements:

- Designation positions
- Clearance (access) to classified information/material
- Investigative requirements
- Adjudication
- Continuous Evaluation Program (CEP)

Element 1: Designation of Positions

Every DLA position is assigned a sensitivity designation based on the criterion that best describes the main duties of the job. Position sensitivity is assigned based on the work that is assigned to the organization and incumbent and focuses on the impact to DLA mission and national security.



Within the Department of Defense (DOD), each civilian position is categorized with respect to security sensitivity into one of three groups:

- Critical Sensitive (CS)
- Non-Critical Sensitive (NCS)
- Non-Sensitive (NS)

Generally, CS positions involve the following:

- Access to top secret information

Lesson Content

- Duties demanding the highest degree of public trust
- Duties under special access programs
- Information Technology (IT) I duties

NCS positions typically involve the following:

- Access to secret information
- Duties requiring public trust
- Information Technology (IT) II duties

All other positions not listed above are non-sensitive

Remember: The sensitivity designation applies to the duties of the position, not to the person occupying the position. A position can be sensitive without requiring access to classified information

Element 2: Clearance Level and Access



This element focuses on access to classified information or material that has been designated as classified by an original classification authority. There are three levels of classified information:

- Top Secret (TS)
- Secret (S)
- Confidential (C)

Lesson Content

Element 3: Investigative Requirements



Once an individual has been selected for a position, a personnel security investigation is conducted to collect and evaluate information about the potential incumbent.

No person shall be appointed to a sensitive position as a civilian employee of DLA, authorized access to classified information, or assigned to duties that are subject to investigation under the provisions of DoD 5200.2-R [Department of Defense Personnel Security Program], unless such appointment, access, or assignment is clearly consistent with the interests of national security.

Source: [DLA Instruction, "Personnel Security Program"](#)

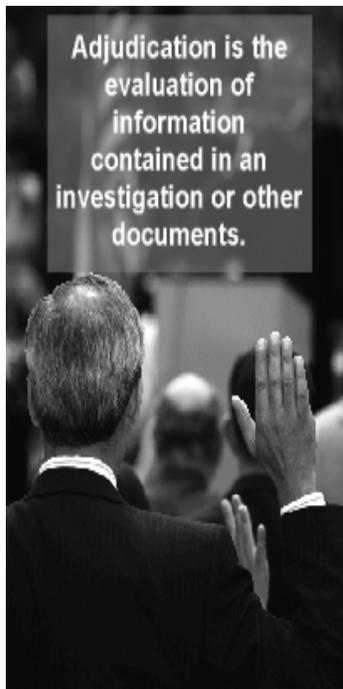
Depending on the sensitivity designation of the positions involved, different types of investigations are initiated. Usually, these investigations must be completed and adjudicated prior to assigning individuals to CS and NCS positions. Depending on the type of investigation and the prospective employee's personal history, the results of the investigation may delay reporting by several months. In some situations, waivers may be possible. More information on Investigations is included in the next section of this course.

Position Sensitivity	Investigative Type
Critical Sensitive (CS)	Single Scope Background Investigation (SSBI)
Non-Critical Sensitive (NCS)	National Agency Check with Written Inquiries (NACI)
Non-Sensitive (NS)	National Agency Check with Written Inquiries (NACI)

Lesson Content

Sources of information for these investigations (and reinvestigations) might include:

- Current and former supervisors
- Co-workers
- Private sources
- Other Government agencies
- Public media
- Activity records
- Individuals occupying other sensitive position and/or clearances



Element 4: Adjudication

Adjudication is the evaluation of information contained in an investigation or other documents. A judgment concerning security eligibility is made by evaluating the information against the DOD Adjudicative Standards. More information about adjudication guidelines and standards is included in the next section of this course. Adjudicative determinations for DLA civilian employees are made by the Washington Headquarters Services, Consolidated Adjudications Facility (WHS/CAF).

Lesson Content

Element 5: Continuous Evaluation Program (CEP)

Once the initial adjudication has been determined, an individual falls under



the Continuous Evaluation Program (CEP) while “in status” (assigned to a sensitive position or having access to classified information or material). By definition, CEP involves the uninterrupted assessment of an individual for retention of a security clearance or continuing assignment to sensitive duties.

CEP includes reinvestigation at given intervals based on the types of duties performed and level of access to secure documents or systems. Incumbents of CS positions are reevaluated every 5 years. Incumbents of NCS positions are reinvestigated every 10 years if they have access to secret material, and every 15 years if the access is to confidential information.

Lesson Content

Investigative and Adjudicative Processes

Introduction

Personnel Security has always and will always be the cornerstone of an effective security program. It is within this security discipline that we find the screening and adjudication process. This process is used to hand pick individuals who are trusted to protect our nation's secrets. It is the process by which an individual's loyalty to the United States is determined. The importance we place on establishing and maintaining an effective personnel security program cannot be overstated.



Source: "Personnel Security – The Cornerstone of Effective Information Protection," Security Education Advisory Council, July 2000.

DLA personnel may be granted a security clearance after a two-step process of investigation and adjudication.

Step 1: Investigation



Investigation involves the inquiry into the employee's past to gather information to help determine whether he or she can be trusted with classified information or to perform sensitive duties.

Lesson Content

As previously discussed, the investigation may involve interviews and record searches.

Investigators may conduct checks in the following areas:

- Financial
- Education
- Criminal
- Drug
- Residences
- Alcohol
- Travel
- Federal Bureau of Investigation (FBI)
- Central Intelligence Agency (CIA)
- Medical
- References

Step 2: Adjudication



Adjudication is the decision whether to grant or deny/revoke either a clearance or the eligibility to perform sensitive duties based upon the investigative evidence.

During the adjudication process, adjudicators use a "whole person" concept in determining whether access is to be granted. They carefully weigh the information that has been gathered during investigation, favorable and unfavorable, past and present. The employee's strengths are evaluated to determine whether these strengths outweigh any weaknesses. Each case is judged on its own merit.

Adjudicative Guidelines

Purpose

A personnel security investigation is an inquiry into an individual's loyalty, character, trustworthiness, and reliability to ensure that he or she is eligible to access classified information or for an appointment to a sensitive position or position of trust. Any doubt concerning personnel being considered for access to classified information/eligibility to perform sensitive duties is resolved in favor of the national security.

Evaluating an individual to determine trust and reliability requires the use of appropriate criteria and standards. Adjudicative Guidelines contained in DOD Regulation 5200.2–R spell out the 13 criteria which adjudicators use when evaluating personnel to make the final determination of trustworthiness, loyalty, and reliability. During the initial clearance/access process, and again on a periodic basis, each candidate is evaluated against the 13 standards of personal conduct. A sufficient period of each person's life is examined to make an affirmative determination that the individual is an acceptable security risk.

Source: "Personnel Security – The Cornerstone of Effective Information Protection," Security Education Advisory Council, July 2000



Evaluating an individual to determine trust and reliability requires the use of appropriate criteria and standards.

Lesson Content

Guidelines

The following are the 13 Adjudicative Guidelines for determining eligibility for access to classified information:

- Allegiance to the United States (U.S.)
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Psychological Conditions
- Criminal Conduct
- Handling Protected Information
- Outside Activities
- Use of Information Technology Systems

Continuous evaluation



To maintain access, employees must recognize and avoid behaviors that might jeopardize their security clearances. Supervisors are well positioned to remind employees of these responsibilities and encourage reporting when an activity or event may put an employee's access or clearance in jeopardy. Early intervention is often the key to quick, effective resolution of problems without harming the employee or the organization.

Lesson Content

Potentially derogatory events

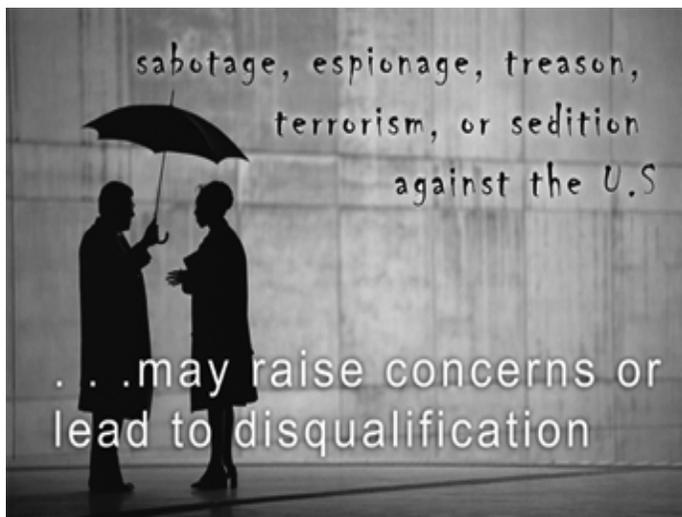
The 13 Adjudicative Guidelines are also used in evaluating the impact of a potentially derogatory event. In addition, the Security Office may take into account other factors:

- The nature, extent, and seriousness of the circumstances
- The fact that reporting was voluntary
- Truthfulness and completeness in responding to questions
- The fact that the employee sought help and followed professional guidance
- Whether positive changes in behavior were demonstrated

Conditions That May Raise Concerns

Introduction

In this section, we will look at each of the 13 Adjudicative Guidelines and examples of conditions that may raise concerns or lead to disqualification.



Lesson Content

Guideline A: Allegiance to the United States (U.S.)

The following are examples of conditions that may raise concerns about allegiance to the U.S.:

- Involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the U.S.
- Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts
- 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 do one of the following:

1) Overthrow or influence the Government of the U.S. 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 U.S. or of any state

Guideline B: Foreign Influence



The following are examples of conditions that may raise concerns about foreign influence:

- 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

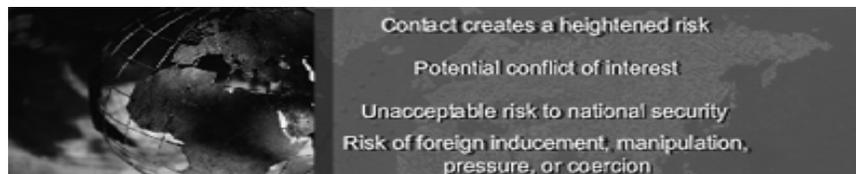
Personnel Security [printable version]

Lesson Content

contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion

- 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
- Counterintelligence information, that may be classified, indicates that the individual's access to protected information may involve unacceptable risk to national security

- 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

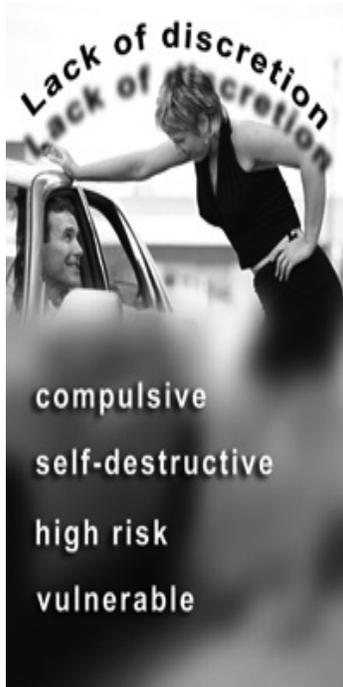


Guideline C: Foreign Preference

The following are examples of conditions that may raise concerns about foreign preference:

- 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
- Action to acquire or obtain recognition of a foreign citizenship by an American citizen
- 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
- Any statement or action that shows allegiance to a country other than the U.S., e.g., renunciation of U.S. citizenship

Lesson Content



Guideline D: Sexual Behavior

The following are examples of conditions that may raise concerns about sexual behavior:

- Sexual behavior of a criminal nature, whether or not the individual has been prosecuted
- 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
- Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress
- Sexual behavior of a public nature and/or that reflects lack of discretion or judgment

Guideline E: Personal Conduct

The following are examples of conditions that may raise concerns about personal conduct:



- 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 employment qualifications award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities
- Deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official Government representative
- Credible adverse information in several adjudicating issue areas that is not sufficient for an adverse determination under any other single guidelines, but

Lesson Content

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

Guideline F: Financial Considerations

The following are examples of conditions that may raise concerns about financial considerations:

- Inability or unwillingness to satisfy debts
- 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
- A history of not meeting financial obligations
- 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

Guideline G: Alcohol Consumption



The following are examples of conditions that may raise concerns about alcohol consumption:

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

Lesson Content

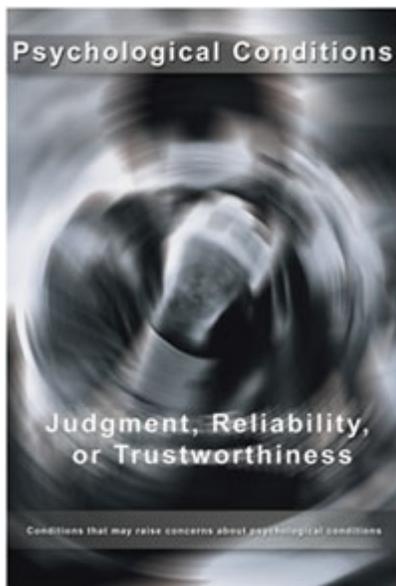


Guideline H: Drug Involvement

The following are examples of conditions that may raise concerns about drug involvement:

- Any drug abuse, i.e., illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction
- Testing positive for illegal drug use
- Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia
- Diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence

Guideline I: Psychological Conditions



The following are examples of conditions that may raise concerns about psychological conditions:

- 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
- An opinion by a duly qualified mental health professional that the individual has a condition not covered under any other guidelines that may impair judgment, reliability, or trustworthiness

Lesson Content

- Failure to follow treatment advice related to a diagnosed emotional, mental or personality condition, e.g., failure to take prescribed medicine

Guideline J: Criminal Conduct



The following are examples of conditions that may raise concerns about criminal conduct:

- A single serious crime or multiple lesser offenses
- Discharge or dismissal from the Armed Forces under dishonorable conditions
- Allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted, or convicted
- Currently being on parole or probation

Guideline K: Handling Protected Information



The following are examples of conditions that may raise concerns about handling protected information:

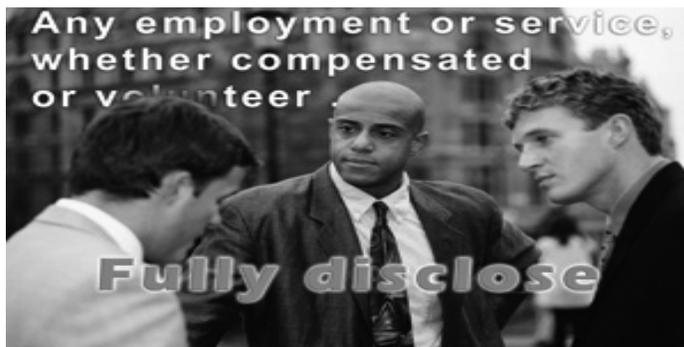
- Deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences
- Collecting or storing classified or other protected information at home or in any other unauthorized location
- 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

Lesson Content

computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment

- Inappropriate efforts to obtain or view classified or other protected information outside one's need to know

Guideline L: Outside Activities



The following are examples of conditions that may raise concerns about outside activities:

- 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, or
 - 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
- Failure to report or fully disclose an outside activity when this is required

Lesson Content

Guideline M: Use of Information Technology Systems

The following are examples of conditions that may raise concerns about misuse of information technology systems:



- Any employment or service, whether compensated or volunteer, with
- Illegal or unauthorized entry into any information technology system or component thereof
- Illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system
- Use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system Downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system

Self-reporting

Self-reporting is an essential component in maintaining the integrity of the Personnel Security Program. Although an employee may obtain a clearance or may be assigned to a sensitive position or position of trust, the initial adjudicative decision can be overturned at a later date if the employee concealed relevant information during the investigation or after the clearance was issued.

Lesson Content



Employees who occupy trusted positions and handle sensitive documents are expected to self-report changes or incidents that may impact their clearances. Once again, the 13 Adjudication Guidelines are a valuable tool in determining if a life-event or situation might result in a need to self-report. Self-reporting, while mandatory, is also a question of personal integrity and certainly preferable to the incident or change being discovered

Listed below are some incidents and life events where self-reporting is expected or may be appropriate.

Change in personal status

Self-reporting may be appropriate for the following types of changes:

- Marital status, e.g., marriage, divorce
- Cohabitation, e.g., living in spouse-like relationship, intimate relationship, engaged
- Change of name

Foreign travel



Self-reporting is appropriate for foreign travel because foreign travel requires the following:

- A security briefing prior to any foreign travel, whether for personal or business reasons
- Clearance for travel to hazardous countries for Sensitive Compartmented Information (SCI)-cleared individuals

Lesson Content

Foreign contacts

Self-reporting is appropriate for the following:

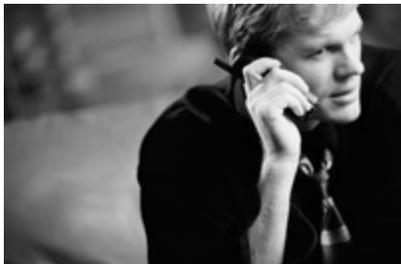
- Contact with individuals of any foreign nationality, either within or outside the scope of your official duties, in which illegal or unauthorized access is sought to classified or otherwise sensitive information
- Personal concern that you are a target of an attempted exploitation
- All close and continuing relationships between SCI-cleared individuals and foreign nationals

Loss or compromise of information

Self-reporting is expected for an inadvertent or accidental loss or compromise of classified or other sensitive information because the first priority in such a situation is to regain control of the classified material.

Financial problems

Self-reporting is appropriate for the following:



- Filing for bankruptcy
- Garnishment of wages
- Having a lien placed on your property for failing to pay a creditor
- Eviction from a residence for failure to pay rent

Lesson Content

Arrests

Self-reporting is appropriate for the following:



- Any arrest, regardless of whether or not charges were filed
- Other involvement with the legal system, e.g., being sued
- Any circumstance where there may be a requirement to discuss job or duties under oath

Psychological counseling

Self-reporting is appropriate for psychological treatment unless it is for marital, family, or grief counseling. Seeking help for routine life crises does not reflect adversely on an individual's judgment. Instead, it may be viewed as a positive sign that an individual recognizes that a problem exists and is willing to take steps toward resolving it.

Role of the supervisor

The ultimate responsibility for maintaining eligibility to access classified or sensitive information rests with the individual employee. However, supervisors are well positioned to provide assurances, an environment that encourages compliance, and ongoing support.



Supervisors and managers play a critical role in assuring the success of the continuous evaluation program. The goal is early detection of an individual's problems. Supervisors are in a unique position to recognize problems early and must react appropriately to ensure balance is maintained regarding the individual's needs and national

Lesson Content

security requirements.

Keys to an active continuous evaluation program are security education and positive reinforcement of reporting requirements in the form of management support, confidentiality, and employee assistance referrals.

Source: Department of the Navy, SECNAVINST 5510.30B

Responsibilities of DLA leaders

DLA leaders, supervisors, and managers, have the following responsibilities:

- Designate civilian positions with appropriate sensitive classification and regularly review those designations to ensure the degree of sensitivity and number of sensitive positions are held to a minimum, consistent with the efficient conduct of business.
- Review the number and level of clearances required to encourage the minimum, consistent with a strict determination of "need-to-know" in the performance of individual employees' official duties.
- Ensure that, when hiring or assigning new duties, the required clearance eligibility is requested in a timely fashion.
- Approve requirements for access to classified information to only those employees who hold the appropriate clearances, ensuring that they are appropriately briefed and debriefed.
- Debrief employees and report to DLA Enterprise Support (DES) when a need for clearance is terminated (without prejudice, when no longer required) or temporarily suspended (when information becomes known that raises doubts about the wisdom of continued security eligibility).
- Maintain an environment where security is known to be important and compliance is expected and required.
- Be aware of situations that may impact the individual's clearance eligibility.
- Provide ongoing training for employees in the proper handling of classified or sensitive material.

- End -