

SECURITY BRIEFING

(Indoctrination for Employees Without Security Clearances) Basic Safeguards and Fundamental Principles of Security Education

This is a preliminary briefing on your security responsibilities, regardless of whether or not you require access to classified information in your job. Simply, we are trying to prevent the disclosure of defense information (including unclassified information) to the wrong people. To prevent this, we have adopted certain safeguards which are used in the receipt, transmission, storage, and even in the destruction of classified information.

Information of the Department of Defense relating to national security shall be protected against unauthorized disclosure as long as required by national security considerations. AR 380-5 establishes a system for classification, downgrading, and declassification of information; sets forth policies and procedures to safeguard such information; and provides for oversight and administrative sanctions for violations. (Para 1-200).

AR 380-5 applies to all military and civilian members of the United States Army. Any violation of its requirements may subject service members to disciplinary actions under Article 92, Uniform Code of Military Justice; civilian personnel are subject to adverse actions under Civilian Personnel Regulations. (Para 1-201).

The varying degrees of classified defense information are defined, in order of importance, with the impact upon national defense should the material be disclosed. An unauthorized disclosure which effects the national security shall be classified in one of three designations: "Top Secret," "Secret," or "Confidential."

TOP SECRET. "Top Secret" shall be applied only to information or material, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

SECRET. "Secret" shall be applied only to information or material, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include: disruption of foreign relations significantly affecting the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security. (Para 1-502).

CONFIDENTIAL. "Confidential" shall be applied to information or material, the unauthorized disclosure of which could reasonably be expected to cause identifiable damage to the national security. Examples of "identifiable damage" include: the compromise of information that indicates strength of ground, air, and naval forces in the United States and overseas areas; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; revelation of performance characteristics, test data, design and production data on munitions of war. (Para 1-503).

There is another protective term common to the Government Services -- "For Official Use Only." This caveat is never used on classified defense information. This caveat is used to protect unclassified information pertaining to individuals, investigative reports, bids, estimates, and budgetary data. There are specific regulations governing the handling and storage of "For Official Use" data, and while the regulations are not nearly as rigid as they are for the classified defense information, this information is limited to U.S. Government employees and it will not be released to the general public.

Employees are placed in positions known as "Nonsensitive," "Sensitive Non-Critical," or "Sensitive Critical." As a new employee, you will normally find yourself in a Nonsensitive position. However, should it become necessary for you to handle classified material, your supervisor will take the necessary steps to obtain a security clearance for you. Based upon the type of investigation completed, the results thereof, and the type of position you assume, a Security Clearance Certificate will be issued and becomes part of your 201 personnel file.

As a new employee, and even though your duties do not require you to handle classified material, at the present time you must be aware at all times of the necessity of the full-time protection of such information.

Should you inadvertently come in contact with classified material or discover a security container open and unattended, you must immediately report this to your supervisor. If your supervisor is not present, call the Security Manager. You must keep the material and/or container under constant surveillance until a responsible person arrives.

Lastly, it is your obligation as a Government employee to ensure protection of our vital defense information, regardless of time, place, or type of position you may occupy. As a new employee, this document has tried to acquaint you with your security responsibilities in as brief a manner as possible. If you are placed in a sensitive position and require access to classified information, you will receive a more detailed indoctrination.

NOTE: OPERATING OFFICIALS WILL ENSURE THE ABOVE INDOCTRINATION IS MADE A MATTER OF RECORD BY ENTERING ON EMPLOYEE RECORD CARD, STANDARD FORM 7-B.

SIGNATURE: _____ DATE: _____