# INTRODUCTION

The granting of a Secret clearance constitutes recognition of the fact that the US Government considers you eligible for access to Secret material and that your character, integrity, and loyalty are above reproach. When you have a “need-to-know” you will be given access to, vital and carefully protected defense information.

All classified material must be protected in accordance with US Government Industrial Security Regulations and LEIDOS procedures. However, Secret material is so sensitive that the stringent rules have been formulated for its handling care. Our Cognizant Security Office scrutinizes our operations very closely for strict compliance with these procedures.

The Department of Defense (DoD) defines SECRET information as follows:

“SECRET” is the designation that shall be applied only to information or material of which the unauthorized disclosure of could reasonably be expected to cause grave damage to the national security. This includes: armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic, and communications intelligence systems; the revelation of sensitive intelligence operations; the disclosure of scientific or technological developments vital to national security.

Government regulations require that you, as an employee/consultant to LEIDOS, be individually warned that you may not disclose SECRET information to any person whose duties do not clearly require a knowledge of the information and then only after you have determined that the person has a SECRET clearance through the Security Department. You may verify the clearance level of any employee through the Security Department when it becomes necessary for you to grant access to SECRET information. It is your responsibility to establish that the intended recipient has the “need-to-know” (Normally, the authority for the decision on the “need-to-know” is vested in the Principal Investigator or the Program Manager). The object of these and other safeguards is to insure that the number of persons given access to SECRET information be kept to an absolute minimum.

**ACCOUNTING**

All SECRET material shall be entered in Document Control’s accountability system when the first of any of the following events occurs:

• The document is retained after the next successive stage in its development is completed (for example: notes converted to draft, final draft placed on masters, or photographic prints developed from negatives).

• The document, including classified working papers and draft, is received in any form at the facility.

• Working papers or drafts are retained for more than 180 days from establishment.

• The document is reproduced for internal purposes (for example: draft review or coordination prior to preparation of final copy).

• The document, regardless of its stage of development, is to be transmitted outside of the facility on a temporary or permanent basis. The transmittal of custody of SECRET material must be covered by a continuous receipt system both within and without the facility.

• All SECRET waste material must be returned in to the Security Department for documentation and destruction on the date it is generated.

All employees cleared for SECRET should be thoroughly familiar with the contents of SECRET material. At the time you generate SECRET material, please call the Security Department to assure that all SECRET control systems procedures are being followed.

# TRANSMITTAL

All SECRET material must be transmitted through, and by, the Security Department. This includes transmittal to another or between LEIDOS and other facilities or User Agencies. Transmittal means a change in physical custody of material. SECRET material being hand carried within LEIDOS must be addressed and securely wrapped to prevent visual access. When practicable, SECRET information should be furnished orally without the physical transmittal of material. At no time should classified material of any level be discussed on unsecured telephones, in public conveyances or places, or in any other manner, that permits interception by unauthorized persons.

**STORAGE**

When not in actual use, SECRET documents must remain the physical control of the Security Department or in safes or rooms approved by the Security Department., unless in an area approved by the Security Department in advance. They cannot be locked in other containers and left unattended at any time.

**REPRODUCTION**

Reproduction of SECRET documents must be made and arranged for by the Security Department. Some SECRET information cannot be reproduced in whole or in part without prior written authority of the Contracting Officer. The need for reproduction of SECRET material must be justified to the Security Department who will obtain the Contracting Officer’s written approval. All reproduction must be done via the Security department so they have records of all copies.

**MARKINGS**

SECRET documents, like all other classified documents, must be properly marked with classification markings as appropriate. As a minimum, the classification must be marked on the outside of file folders and folded maps or charts. All SECRET material must show the date of origin and downgrading information when required, and each paragraph must be marked with its specific classification including lead-in paragraphs and subparagraphs.

**DESTRUCTION**

All SECRET material, including waste material, must be accounted for and destroyed only by the personnel of the Security Department.

**LOSS, COMPROMISE, OR VIOLATIONS**

Any loss, compromise, or violation of regulations governing the handling of SECRET information must be reported immediately to the Manager DoD/DOE Security Programs so that the required action and report to the Cognizant Security Office may be made.

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ attest that I have received the LEIDOS Secret Briefing. I understand the additional requirements for all individuals who are afforded access to Secret information or material. I further acknowledge that I will comply with the Secret requirements as outlined in the NISPOM.

**IN-BRIEFING:**  **EXIT-BRIEFING:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Briefed Date Debriefed

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Employee Signature of Employee

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee # Employee #

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Name/Signature of Briefer Name/Signature of Debriefer