

**Security Indoctrination Briefing**

**General Information**

As a Defense Contractor, KGH is required by the Defense Security Service (DSS), in accordance with our Security Agreement, to give a security indoctrination to all personnel before allowing them access to classified information. In accordance with this agreement, our company has been granted a facility security clearance at the level of Top Secret. We are required to install and maintain comprehensive security measures for the protection of classified information developed by or furnished to us. It is the personal responsibility of every employee who handles, or otherwise comes in contact with classified information, to observe at all times our written company security procedures and other instructions as may be issued by the Security Office.

**National Industrial Security Program (NISP) Overview**

The NISP is the U.S. government’s industry program to safeguard classified information that has been entrusted to industry in conjunction with defense contracts. DSS, on behalf of the Department of Defense (DoD), has been delegated the security administrative responsibilities for these classified contracts. This means that DSS will provide advice, assistance, and ensure compliance with all applicable requirements of the National Industrial Security Program Operating Manual (NISPOM) that affect our classified program(s).

The NISP is commonly administered within each cleared facility by the Facility Security Officer (FSO). Top management is ultimately responsible for administration of the classified program, but this authority is generally delegated to the FSO. The FSO is responsible for all security matters relative to the safeguarding and handling of classified information.

The NISPOM, established by Executive Order 12829 dated 06 January 1993, is industry’s primary reference in the protection of classified information. This manual outlines the proper procedures for handling and safeguarding information classified pursuant to Executive Order 12958, as amended. It provides uniform rules for all industrial companies under the NISP, and each company working on any government classified contract must comply with its provisions.

Companies with classified DoD contracts require facility security clearances, which are granted and administered by DSS. The DSS is responsible for ensuring compliance with the NISPOM, and it does this by conducting regular security reviews at all cleared companies.

These reviews are normally all encompassing and tend to include a review of the company’s security procedures to include, if applicable, the Standard Practice Procedures (SPP), accredited information systems, classified visits, security education, and safeguarding and handling of classified information.

DSS has the authority to suspend or revoke a facility clearance if it finds that the company’s security procedures are unsatisfactory for handling and safeguarding classified information. The DSS rating of unsatisfactory can negatively impact a company’s ability to conduct future classified work. Consequently, poor security practices are not only detrimental to the national security, but they may have a direct impact on all employees’ jobs and the company’s ability to perform on classified contracts.

**SF-312**

NISPOM Paragraph 3-105 requires that an individual issued an initial personnel security clearance (PCL) execute a Classified Information Nondisclosure Agreement (SF-312) prior to being granted access to classified information and that the completed form is forwarded to the Cognizant Security Agency for retention. This agreement is legally binding, outlining your obligations in having access to and protecting classified information.

**Classified Information**

Classified information is official government information that has been determined to require protection in the interest of national security. All classified information is under the sole ownership of the U.S. government and, as such, employees possess no right, interest, title, or claim to such information. (There is one exception: information developed under an Independent Research & Development (IR&D) Program).

Classified information exists in many forms. It may be a piece of hardware, photograph, film, recording tapes, notes, drawing, document, or spoken words. Classified material is marked as such upon origination. It comes to industry via a DD Form 254, security classification guides or classified source materials. The degree of safeguarding required depends on its classification category. Three levels of classification have been established based on their criticality to national security:

TOP SECRET: Information or material whose unauthorized disclosure could be expected to cause exceptionally grave damage to national security

SECRET: Information or material whose unauthorized disclosure could be expected to cause serious damage to national security

CONFIDENTIAL: Information or material whose unauthorized disclosure could be expected to cause damage to national security

DSS has security cognizance over DoD classified information bearing any of these three classification levels. There are also other categories of classified information that require special access authorization. The customer will provide information concerning these. You may hear terms such as Sensitive Compartmented Information (SCI), or Special Access Program (SAP). Information pertaining to these programs will be provided if you are assigned to work with these programs.

There are other categories of information, which, while not classified, deserve mention. **For Official Use Only (FOUO)** and **Sensitive But Unclassified (SBU)**, to name a few, is unclassified information which is exempt from general public disclosure and must not be given general circulation.

As a minimum, after the determination of the level of classification, classified material shall be marked with the date of origin, the name and address of the facility responsible for its preparation, and be plainly and conspicuously marked, stamped, or typed with the appropriate classification level at the top and bottom of each page, front and back. Each portion, section, part, paragraph, or similar portion of a classified document shall be marked to show the level of classification.

In addition to government classified information, KGH produces company private or proprietary information. This information is not to be divulged to individuals outside of the company. Examples of this information are salary and wage lists, technical and research data, and proposals. Employees should protect this information in such a manner as to preclude unauthorized access. This information can be marked Company Confidential or Company Private. Caution should be taken to keep this information separate from U.S. government classified information.

**Access Requirements and Need-to-Know**

Access to classified information occurs when a person has the ability and opportunity to obtain knowledge of the classified information. Authorized access to classified information may be granted only when two conditions are met: First, the recipient must have a valid and current security clearance (eligibility and access in JPAS) at a level at least as high as the information to be released. Second, the recipient must demonstrate the need for access to the classified information. This is referred to as **need-to-know**.

Need-to-know is met when access to classified information by an individual is essential to the performance of his or her job duties in fulfilling a classified contract. Each individual, regardless of rank, position, or amount of clearances and accesses, only has a need-to-know for information pertinent to the performance of his or her specific program. Need-to-know is not the same as want-to-know. Individuals must always establish a person’s need-to-know before sharing classified information.

It is the responsibility of the holder of the classified information to ensure the proper clearance and need-to-know of the recipient. The possessor must also advise the recipient of the classification of the information disclosed.

Need-to-know confirmation should come from a security representative. If there is doubt as to whether or not a person has a need-to-know, the employee should check with the security prior to the release of any classified information. Establishment of need-to-know is critical. It is far better to delay release to an authorized person than to disclose classified information to an unauthorized individual.

**Safeguarding Classified & Sensitive Information**

One of the most fundamental requirements of the NISP pertains to the proper safeguarding and storage of classified information. **KGH facilities are not approved for classified storage.** Therefore, no **physical** classified information should come in or go out of the facility. Classified discussions, however, may take place. It is essential that classified information be properly safeguarded in accordance with the requirements of the NISPOM at all times.

Classified discussions must take place in a secure, preferably closed-door, area. This will prevent any unauthorized persons from over-hearing information. The area must be approved for classified discussion. Please contact FSO or CEO for further information.

When working with sensitive, unclassified material, you should store the documents in a container, or properly cover, when you leave your desk. Lock your computer screen when not attended. Make sure to log off of your computer, and lock all drawers and cabinets, when leaving the office for the day.

**Transmittal/Reproduction/Destruction of Classified Material**

For questions concerning transmittal, you should contact the FSO. Safeguarding of classified material is not approved at KGH facilities. No employee or visitor is allowed to bring classified material in or out of KGH offices. Reproduction/destruction of classified material is prohibited in KGH facilities.

**Classified Visits**

All classified visits must be coordinated through your local Security Representative. A Visit Authorization Request must be completed and forwarded to the appropriate Security Officer before you can visit another contractor facility or government agency on a classified visit. Contact your FSO if you need further instruction.

Classified meetings within facilities should be in areas in which the information being discussed cannot be overheard by unauthorized persons. If the classified meeting is between employees, it is the responsibility of the meeting sponsor to verify the need-to-know and the clearances of all attendees.

Classified telephone discussions can only be had via the use of a Secure Telephone Unit (STU-III). **Do not** discuss classified information on phones not approved for its discussion.

**Employee Reporting Requirements**

Employee-reporting is a critical element in the NISP. It is your responsibility to report, to your Security Office, the below:

* Suspicious Contacts
* Security Violations
* Adverse Information
* Change in Name/Citizenship/Job Status/Marital Status
* Unauthorized receipt of classified material
* Loss, compromise, or suspected compromise of classified information
* Acts (or attempted acts) of sabotage, espionage, and any other subversive activity

**Termination of Employment**

As a cleared employee, you have a responsibility to surrender all security-related material in your possession to the Security Officer upon termination. In addition, you must sign and date a Debriefing Form and return your badge prior to departure.

**KGH Security Contact information:**

FSO – Janet Glasby – glasby@kiernan.co

AFSO – Sheri Donahue - sheri.donahue@att.net