



SECURITY INDOCTRINATION BRIEFING

GENERAL INFORMATION

Foreign Disclosure & Export Solutions Corporation, as a Defense Contractor, 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 SECRET. We are required to install and maintain comprehensive security measures for the protection of classified material 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 any other instructions as may be issued by the Security Office.

NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) OVERVIEW

The NISP is the U.S. government-industry program designed to safeguard classified information that has been entrusted to industry in conjunction with defense contracts. It may be envisioned as the three-way partnership, in which the government customer or user agency enters into a classified contractual agreement with a cleared industrial facility and DSS oversees and validates compliance with security portions of that contract. The government has established the DSS to provide advice, assistance, and supervision of program elements, and has developed a set of rules and requirements contained in the National Industrial Security Program Operating Manual (NISPOM).

The NISP is commonly administered within each cleared facility by the Facility Security Officer (FSO). Top management is ultimately responsible for administration of the 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. The NISPOM outlines the proper procedures for handling and safeguarding information classified pursuant to Executive Order 12958. It provides uniform rules for all industrial firms under the NISP, and each firm working on any government- classified contract must comply with its provisions.

Facilities with classified DoD contracts require facility security clearances, which are granted and administered by DSS. They are responsible for ensuring compliance with the NISPOM, and it does this principally by conducting regular security reviews at all cleared facilities. These reviews are normally all encompassing and tend to include a review of the company's Security Practices & Procedures (SPP), information management system, classified material accountability, and safeguarding and handling of classified information. The level and amount of classified material possessed at a facility normally determine the frequency and length of such inspections. 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. DSS ratings of unsatisfactory will negatively impact a facility'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 company's ability to perform on classified contracts.

CLASSIFIED INFORMATION DEFINITION AND DESCRIPTION

Classified information is official government information that has been determined to require protection in the interest of national security. All classified information is under sole ownership of the U.S. government, and as such employees possess no right, interest, title, or claim to such information.

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

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

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

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

DSS has security cognizance over DoD classified material of information and their three levels of classification. 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 the company is cleared to these levels and if you are assigned to work with these programs.

There are other categories of information, which, while not classified, also deserve mention. For Official Use Only (FOUO) is unclassified DoD 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 shall be plainly and conspicuously marked, stamped or typed with the appropriate classification at the top and bottom of each page, front and back. Each portion, section, part, paragraph, or similar portions of a classified document shall be marked to show the level of classification. The FSO must approve the classified markings prior to submission to a customer or other agency.

In addition to government classified information, Foreign Disclosure & Export Solutions Corporation produces a large amount of company private or proprietary information. This business 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, trade secrets and proposals. Employees should protect this information in such a manner as to preclude unauthorized access. This information can be marked Company Confidential or Secret. 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 classified information. Authorized access to classified information may be granted only when three conditions are met: First, the recipient must have a valid and current security clearance eligibility 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. Finally, the recipient must have a bona fide 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 task or project. 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 possessor of 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 department advisor or representative. If there is doubt as to whether or not a person has a need-to-know, the employee should check with the proper authority prior to release of any classified information. Establishment of need-to-know is essential. It is far better to delay release to an authorized person than to disclose classified information to an unauthorized individual.

SAFEGUARDING CLASSIFIED INFORMATION

One of the most fundamental requirements of the NISP pertains to the proper safeguarding and storage of classified information. It is essential that classified information be properly safeguarded or stored in accordance with the requirements of NISPOM at all times. A natural way of approaching the subject of safeguarding is to divide it into requirements for safeguarding when classified materials are in use and when not in use.

WHEN IN USE

While in use, classified material must never be left unsecured or unattended. An authorized individual who is able to exercise direct control over the classified material must keep it under

constant surveillance. The authorized individual must have the appropriate eligibility, access and need-to-know, and must take action to prevent access to the material when others who do not have the appropriate clearance and need-to-know are present.

When working with classified material in an unsecured area, any open curtains or doors should be closed. It is prudent to also post a sign, declaring “CLASSIFIED WORK IN PROGRESS”. If a visitor or unauthorized employee is present, a classified document must be protected by either covering it, turning it face down, or placing it in an approved storage container.

When working on classified material you must lock the documents in an approved storage container when you leave your desk for lunch or coffee/smoke breaks. They must never be tucked in a desk drawer, file cabinet, credenza, key-lock file, etc., for even the briefest period. This rule also covers typewriter ribbons being used for classified material. If you are working on a computer and need to take a break, you must comply with AIS procedures. You cannot just turn off your computer and expect the classified information to be safe. Classified information should be stored as soon as possible after it has been used.

WHEN NOT IN USE

When not in use, classified material must be properly secured in the company’s approved classified storage container, unless another properly cleared person with a need-to-know is guarding it. The storage of classified material in anything other than an approved container is strictly prohibited.

Approved storage containers must remain in a locked position unless they are under constant surveillance and control. The employee should always shield the combination from the sight of others when opening a classified container. Combination padlocks must be stored inside or locked on the container when it is open. This prevents tampering or replacement of the padlock by an unauthorized person.

Combinations to classified storage containers and controlled areas are themselves classified and must therefore be protected at the same level of the data they are protecting. Combinations to classified containers must be committed to memory. They cannot be written on slips of paper to be kept in desks, wallets, notebooks, etc. In addition, they cannot be written down in a coded form, such as backwards, out of order, etc. Only in certain circumstances can combinations be written down and safeguarded as a piece of classified material. In choosing a combination, employees should avoid persons, places or things that can be easily identified with them, such as a birthday, spouse’s name, favorite sports team, license plate, etc. At many facilities, there is a strict prohibition against sharing safe combinations, since only those authorized to have access to the container may know the combination. Combinations must be changed whenever anyone with access leaves the organization or transfers to another group.

If circumstances prevent you from storing material in the prescribed container you should inform the FSO and hold the material until he or she arrives and takes control of the material.

TRANSMITTAL OF CLASSIFIED MATERIAL

The transmittal of classified material will generally be performed by the FSO. For Questions concerning transmittal you should contact the FSO. No employee or visitor is allowed to bring classified material in or out of Foreign Disclosure & Export Solutions Corporation facilities without first logging in the material via the FSO.

Each cleared facility within the Foreign Disclosure & Export Solutions Corporation organization is required to maintain complete records for all classified material in its possession. All classified information will be logged on the Information Management System.

Methods for transmittal of classified information depend on the material's classification and its destination. The FSO will insure that the material is properly packaged and transmitted in accordance with the NISPOM.

REPRODUCTION

Prior to reproducing and classified information, check with the FSO. Each copy made must be entered into the Information Management System and all waste disposed of properly. Only certain copying machines are authorized for use. Additional information and procedures will be explained by the Facility Security Officer at the time reproduction is required. Remember that the reproduction of classified information will be held to a minimum.

DESTRUCTION

When it is determined that a piece of classified information is no longer required, it should be destroyed. Material to be destroyed will be entered on a destruction report and destroyed in a manner approved by DSS. A witness, while not required for material classified Secret or below, should be used. Some destruction reports attached to material received from DoD require a witness sign the form. The FSO should review material logged on the Information Management System on a yearly basis and destroy any material not required.

EMPLOYEE REPORTING REQUIREMENTS

The NISP is based to a large extent on individual trust and responsibility, and employee-reporting requirements are a critical element in the program. Employees are required to report any suspicious occurrences, known security infractions, adverse information and any change in employee status. Employee reporting requirements are designed to protect the employee and counter any possible hostile intelligence threat. It is your personal responsibility to understand and report these conditions to the security office as circumstances warrant.

SUSPICIOUS OCCURRENCES

Employees are required to report any suspicious behavior or occurrences that may occur at any time. More specifically, employees must report to the FSO any of the following events:

- 1) Any efforts, by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified or sensitive information.
- 2) Any efforts, by any individual, regardless of nationality, to compromise a cleared employee.
- 3) Any contact by a cleared employee with a known or suspected intelligence officer from any country.
- 4) Any contact, which suggests the employee concerned, may be the target of any attempted exploitation by the intelligence services of another country.

If there is any question as to whether any specific situation is reportable, it too should be reported.

SECURITY VIOLATIONS OR INFRACTIONS

Employees are required to report known or suspected security violations to the FSO. Reporting provides employees with an opportunity to extricate themselves from a compromising situation and enhances the protection of national security information. Ideally, Foreign Disclosure & Export Solutions Corporation security posture should be enhanced as the result of a security infraction, because security professionals will have an opportunity to address and correct any problems that may exist. When an employee covers up a known security infraction, the security education process is negated because security is denied the chance to rectify deficiencies. The relationship of mutual trust between the contractor and the DSS is also jeopardized. In addition, not reporting a known security violation may constitute a major security violation itself, regardless of the severity of the unreported incident. Some common security violations are:

- 1) Classified material left out or unattended.
- 2) Unsecured, unattended security containers/unsecured combinations.
- 3) Removal of material without approval.
- 4) Lost classified information.
- 5) Unauthorized copying or destroying classified material.
- 6) Unauthorized/improper transmission of classified material.
- 7) Disclosure of/permitting access by an unauthorized person.
- 8) Processing classified material on a non-approved computer.

ADVERSE INFORMATION

The NISPOM requires that cleared defense contractor employees report to their respective security department adverse information regarding other cleared employees. As a general rule,

adverse information is that which reflects unfavorably on the trustworthiness or reliability of the employee and suggests that their ability to safeguard classified information may be impaired. Examples of this include: excessive indebtedness or recurring financial problems, unexplained affluence, use of drugs or excessive use of intoxicants, bizarre behavior, mental or emotional problems, and criminal behavior. Wage garnishments are considered adverse information that needs to be reported.

Reporting adverse information on coworkers is one of the most difficult tasks you may have. Employees find it difficult to be objective in assessing the impact of personal problems on job performance or continuing clearance eligibility. Many employees feel by reporting such behavior they are playing a policing role, a role, they have no desire to perform. Other employees may take too zealously to this reporting requirement. Employees are cautioned against creating an atmosphere of suspicion or intrusiveness in the work place. Employees should be more concerned with their own work than that of others, but at the same time they should be vigilant and not turn a blind eye to the questionable behavior or practices of coworkers.

Employees found to have a problem with drugs or intoxicants will be processed in accordance with legal constraints and Foreign Disclosure & Export Solutions Corporation policies and procedures relating to employee support.

Adverse information should be reported to protect the individual from being placed in a position where he or she could be exploited and persuaded to commit a security violation, or even espionage. Many espionage cases can be cited in which hostile intelligence agents exploited a human weakness. If you are unsure if certain behavior requires reporting, you should consult the FSO for guidance.

REQUIRED REPORTS

Cleared employees are required to report any information pertaining to the following events directly to the FSO.

- 1) Foreign travel to or through a country that is overtly hostile to the US or attendance at international conferences at which representatives of such a country were or will be in attendance.
- 2) Establishment of residency in an overtly hostile country by an employee's spouse or member of his/her immediate family or the acquisition of relatives, through marriage, who live in such a country.
- 3) Any loss, compromise, or suspected compromise of classified information in your possession or in the possession of another person.
- 4) Any association with or intention to represent a foreign interest (RFI).
- 5) Change in name, residence or marital status.
- 6) Receipt of classified material not related to a classified contract, project, or program for which no safeguarding or disposition instructions have been received.
- 7) Any instances in which classified material is out of the control of the custodian or which cannot be readily located.
- 8) Any instances, in which an employee desires not to perform on classified work, accept

security responsibility, or requests to terminate clearance or clearance processing.

9) Any instances in which someone approaches you and requests information pertaining to classified information when such person does not have a legitimate “need-to-know” and/or is willing to “pay” you for such information.

10) The experience of grave financial problems or lawsuits.

OTHER REPORTING REQUIREMENTS

In addition to the above, employees are required to report any act of sabotage or possible sabotage, espionage or attempted espionage, and any subversive or suspicious activity. You are also encouraged to report any attempts to solicit classified information, unauthorized persons on company property, and disclosure of classified information to an unauthorized person, along with any other condition that would qualify as a security violation or which common sense would dictate as worth reporting.

SECURITY VIOLATIONS

Foreign Disclosure & Export Solutions Corporation has established strict disciplinary action procedures for employees who knowingly and willingly violate the security procedures outlined in the Corporate SPP. Repeated violations of the security procedures may result in termination of employment. Some common examples of security violations are security containers left unattended; unsecured combinations; removal of classified material without approval; lost classified information; copying or destroying classified material without approval; unauthorized/improper transmission of classified material; and, disclosure of/permitting access to classified information to an unauthorized person.

TERMINATION OF EMPLOYEMENT

As a cleared employee, you have a responsibility to surrender all classified material in your possession to the FSO upon termination. In addition, you must sign and date a Debriefing Form and return your company identification badge prior to departure.

SECURITY PRACTICES & PROCEDURES

The FSO publishes a procedural manual, the Security Practices & Procedures (SPP), which outlines the security procedures in greater detail. All cleared employees who handle classified material are required to read and understand the SPP. It may be found on the company’s website under “Employees Only” at the bottom of the fdesolutions.com home page.

EMPLOYEE ACKNOWLEDGEMENT

This completes the Foreign Disclosure & Export Solutions Corporation Security Indoctrination Briefing. Should you have any questions, please call or talk to the Facility Security Officer. You are encouraged to print out a copy of this briefing for your records, and you should refer to it, the company’s Security Practices & Procedures document, and the NISPOM for further guidance. When in doubt, ask the FSO prior to taking any action that may jeopardize your personal security clearance or the company’s facility security clearance.