

**STANDARD PRACTICE PROCEDURES FOR SECURITY**

***(This document conforms to the requirements of the NISPOM dated January 1995)***

TABLE OF CONTENTS

[SECTION I 6](#_Toc357498591)

[WHY IMPLEMENT STANDARD PRACTICE PROCEDURES? 6](#_Toc357498592)

[SECTION 2 7](#_Toc357498593)

[GENERAL INFORMATION 7](#_Toc357498594)

[A. Hotline Numbers 7](#_Toc357498595)

[B. Cooperation with DSS Agents and Other Federal Agencies 7](#_Toc357498596)

[C. The Defense Security Service 8](#_Toc357498597)

[D. Loss, Compromise, or Suspected Compromise of Classified Information and Handling Security Violations 9](#_Toc357498598)

[E. Disciplinary Actions Related to Security Violations 10](#_Toc357498599)

[SECTION 3 11](#_Toc357498600)

[INDIVIDUAL RESPONSIBILITIES 11](#_Toc357498601)

[A. Safeguarding Classified Information 11](#_Toc357498602)

[B. Reporting Information 12](#_Toc357498603)

[C. Responsibilities of Supervisors and Managers 13](#_Toc357498604)

[SECTION 4 14](#_Toc357498605)

[THE FACILITY SECURITY OFFICER 14](#_Toc357498606)

[A. FSO’s Responsibilities 14](#_Toc357498607)

[SECTION 5 16](#_Toc357498608)

[PERSONNEL SECURITY CLEARANCES 16](#_Toc357498609)

[A. Request for a Security Clearance 16](#_Toc357498610)

[B. Application for a Security Clearance 16](#_Toc357498611)

[C. Processing a Security Clearance 20](#_Toc357498612)

[D. Termination of a Security Clearance 22](#_Toc357498613)

[SECTION 6 22](#_Toc357498614)

[SECURITY EDUCATION 22](#_Toc357498615)

[A. Initial Security Briefing 22](#_Toc357498616)

[B. Refresher Security Briefing 23](#_Toc357498617)

[C. Threat Awareness Briefing 24](#_Toc357498618)

[D. Defensive Security Briefing 25](#_Toc357498619)

[E. Debriefings 28](#_Toc357498620)

[SECTION 7 28](#_Toc357498621)

[CLASSIFIED VISITS 28](#_Toc357498622)

[A. Incoming Visits 28](#_Toc357498623)

[B. Outgoing Visits 29](#_Toc357498624)

[C. Meetings 30](#_Toc357498625)

[SECTION 8 30](#_Toc357498626)

[STORAGE OF CLASSIFIED MATERIAL 30](#_Toc357498627)

[A. Automated Information Systems 31](#_Toc357498628)

[SECTION 9 32](#_Toc357498629)

[CONTROL OF CLASSIFIED MATERIAL 32](#_Toc357498630)

[SECTION 10 33](#_Toc357498631)

[TRANSMISSION OF CLASSIFIED MATERIAL 33](#_Toc357498632)

[A. Transmission of Classified Material Outside the Facility 33](#_Toc357498633)

[B. Courier Procedures and Courier Briefing 34](#_Toc357498634)

[SECTION 11 36](#_Toc357498635)

[CLASSIFICATION AND ORIGINATION OF CLASSIFIED MATERIAL 36](#_Toc357498636)

[A. Origination of Classified Material 36](#_Toc357498637)

[B. The DD Form 254 37](#_Toc357498638)

[SECTION 12 38](#_Toc357498639)

[MARKING CLASSIFIED MATERIAL 38](#_Toc357498640)

[A. Marking Requirements for Information and Material 38](#_Toc357498641)

[B. Marking Specific Types of Material 45](#_Toc357498642)

[C. Marking of Regraded Documents and Material 50](#_Toc357498643)

[D. Marking of Foreign Classified Material 51](#_Toc357498644)

[E. Marking Wholly Unclassified Material 52](#_Toc357498645)

[F. Marking Compilation 52](#_Toc357498646)

[SECTION 13 53](#_Toc357498647)

[DISPOSITION OF CLASSIFIED MATERIAL 53](#_Toc357498648)

[A. Ongoing Program of Reduction 53](#_Toc357498649)

[B. Means of Disposition 53](#_Toc357498650)

[C. Responsibilities for Disposition of Classified Material Related to Solicitations and Contracts 54](#_Toc357498651)

[D. Responsibilities for Disposition of Other Classified Material 55](#_Toc357498652)

[E. Destruction of Classified Material 56](#_Toc357498653)

[SECTION 14 57](#_Toc357498654)

[REPRODUCTION OF CLASSIFIED MATERIAL 57](#_Toc357498655)

[SECTION 15 58](#_Toc357498656)

[REQUIREMENTS FOR TOP SECRET MATERIAL 58](#_Toc357498657)

[A. Control and Accountability 58](#_Toc357498658)

[B. Generation of TOP SECRET Material 58](#_Toc357498659)

[C. Storage of TOP SECRET Material 58](#_Toc357498660)

[D. Transmission of TOP SECRET Material 58](#_Toc357498661)

[E. Reproduction of TOP SECRET material 59](#_Toc357498662)

[F. Disposition of TOP SECRET material 59](#_Toc357498663)

[SECTION 16 59](#_Toc357498664)

[SPECIAL REQUIREMENTS FOR RESTRICTED DATA 59](#_Toc357498665)

[A. Restricted Data and Formerly Restricted Data 59](#_Toc357498666)

[B. DOD Critical Nuclear Weapon Design Information 60](#_Toc357498667)

[C. NATO Information 61](#_Toc357498668)

[D. COMSEC Information 63](#_Toc357498669)

[E. INTELLIGENCE Information 64](#_Toc357498670)

[SECTION 17 64](#_Toc357498671)

[INTERNATIONAL SECURITY REQUIREMENTS 64](#_Toc357498672)

[A. Disclosure of U.S. Information to Foreign Interests 65](#_Toc357498673)

[B. Foreign Government Information 66](#_Toc357498674)

[C. International Transfer of Classified Material 68](#_Toc357498675)

[D. International Visits and Control of Foreign Nationals 68](#_Toc357498676)

[SECTION 18 72](#_Toc357498677)

[EMERGENCY PROCEDURES 72](#_Toc357498678)

[SECTION 19 73](#_Toc357498679)

[SAMPLE SECURITY FORMS 73](#_Toc357498680)

# SECTION I

## WHY IMPLEMENT STANDARD PRACTICE PROCEDURES?

This facility has entered into a Security Agreement with the Department of Defense in order to have access to information that has been classified because of its importance to our nation’s defense.

Some of our programs and activities are vital parts of the defense and security systems of the United States. All of us - both management and individual employee - are responsible for properly safeguarding the classified information entrusted to our care.

Our Standard Practice Procedures conforms to the security requirements set forth in the government manual - the National Industrial Security Program Operating Manual or NISPOM. The purpose of our SPP is to provide our employees with the requirements of the NISPOM as they relate to the type of work we do. This document should also serve as an easy reference when questions about security arise. The NISPOM is available for review by contacting the Facility Security Officer.

Our facility fully supports the National Industrial Security Program. All of us have an obligation to ensure that our security practices contribute to the security of our nation’s classified defense information.

Senior Management Official

# SECTION 2

## GENERAL INFORMATION

A. Hotline Numbers

Federal agencies maintain hotlines to allow an unconstrained avenue for government and contractor personnel to report - without fear of reprisal - any known or suspected instances of security irregularities or infractions concerning defense affiliated contracts, programs or projects.

All contractors still have the responsibility to facilitate reporting and timely investigation of suspected or real security irregularities involving their operations or personnel, and employees are encouraged to furnish information through established company channels.

The addresses and phone numbers for the hotlines are as follows:

|  |  |
| --- | --- |
| CIA HOTLINE  Office of the Inspector General  Central Intelligence Agency  Washington, D.C. 20505  (703) 874-2600 | DEFENSE HOTLINE  The Pentagon  Washington, D.C. 20301-1900  (800) 424-9098  (703) 693-5080 |
| DOE HOTLINE  Department of Energy  Office of the Inspector General  1000 Independence Avenue, S.W.  Room 5A235  Washington, D.C. 20585  (202) 586-4073 or (800) 541-1625 | NRC HOTLINE  U.S. Nuclear Regulatory Commission  Office of the Inspector General  Mail Stop TSD 28  Washington, D.C. 20555-0001  (800) 233-3497 |

B. Cooperation with DSS Agents and Other Federal Agencies

Assistance and cooperation shall be extended to the Defense Security Service and other Federal Agencies, during the conduct of official investigations, including background investigations to determine the eligibility of persons for security clearances, and investigations concerning the unauthorized disclosure of classified information. This cooperation shall include assistance in arranging appointments with employees to be interviewed and providing a space for private interviews, when required.

C. The Defense Security Service

The Defense Security Service or DSS is an agency of the Department of Defense. DSS provides two primary services for many User Agencies of the Government, such as the Departments of the Navy, Air Force and Army. The Personnel Security Investigations Program is responsible for the determination of the eligibility of individuals for a security clearance. Special Agents of DSS may contact you while determining your eligibility for a security clearance or they may contact you in connection with another employee’s security clearance.

The DSS also administers the National Industrial Security Program which was established by Executive Order 12829, January 6, 1993. The NISP is responsible for the determination of the eligibility of contractors for a security clearance, and provides oversight of contractors’ procedures and practices for safeguarding classified defense information. Industrial Security Specialists of DSS may contact you in connection with the conduct of a security review of the facility, an investigation of an unauthorized disclosure of classified information or to provide advice and assistance to you and the company on security related issues.

Our cognizant security office of the DSS is located at:

For all DoD contractors participating in the NISP, DoD will be the CSA, or Cognizant Security Agency. The local DSS FO (Field Office) will be the CSO or Cognizant Security Office for most NISPOM requirements. DISCO or the Defense Industrial Security Clearance Office, may be the CSO for certain security clearance/reporting requirements.

The DSS Counterintelligence or CI Office was established in 1993. Counterintelligence refers to activities conducted to destroy the effectiveness of foreign intelligence operations and to protect information against espionage. The term also refers to information developed by or used in counterintelligence operations. Espionage refers to any clandestine intelligence collection activity. CI was integrated into our overall mission to assist us in ensuring more threat appropriate security systems are created for industry. DSS Industrial Security Specialists are in an excellent position to enhance security while supporting U.S. industry’s business overseas by providing the following services to both cleared contractors and to the Intelligence Community of the U. S.:

1. Assist in the earliest possible detection of potential espionage threats in cleared contractor facilities and to disseminate that information to appropriate Intelligence Agencies of the United States.

2. Help contractors to identify potential espionage or foreign intelligence threats to their facility and to report the information.

3. Help contractors develop threat appropriate countermeasures to foreign intelligence threats.

**UP TO $500,000 REWARD FOR STOPPING ESPIONAGE!**

An amendment to Title 18 U.S.C. Section 3071 recently enacted authorizes the Attorney General to make payment for information which leads to the arrest and conviction of espionage activity in the following areas:

1. In any country, any person(s) for commission of an act of espionage against the United States.

2. In any country, any person(s) for conspiring or attempting to commit an act of espionage against the United States; or

3. Leading to the prevention or frustration of an act of espionage against the United States.

D. Loss, Compromise, or Suspected Compromise of Classified Information and Handling Security Violations

A compromise occurs when classified information is disclosed to a person or persons without the proper level security clearance or need-to-know for the information. Any violation of security program requirements must be reported immediately. Timely reporting of a security violation is critical to ensuring effective follow-up action is taken to limit the damage and to identify the possibility of a compromise of classified information. Failure to report a loss, compromise, suspected compromise, or violation is itself a violation.

Any employee who detects or suspects any of the following incidents must immediately notify our Facility Security Officer:

1. The loss or suspected loss of classified material.

2. The compromise or suspected compromise of classified information.

3. Any violation of a requirement of this manual or of the NISPOM.

Any employee who is traveling outside this facility who believes a loss or compromise of classified information may have or did occur should notify the FSO as soon as possible. If you are within another DoD cleared facility the FSO of that facility should be notified as well. The nearest office of the Defense Security Service should be contacted. If you are in a foreign country the nearest U.S. Government authority should be contacted.

The following information is of key importance when reporting any of the above incidents:

1. What is alleged to have happened, where, and when did it occur?

2. Who reported the incident or violation, to whom and when?

3. What classified information was involved? Provide a list of the material if possible.

4. What was the classification of the information involved?

5. When, for how long, and under what circumstances was classified information vulnerable to unauthorized disclosure?

6. Determine identity of unauthorized individuals likely to have had access to the classified information.

7. What actions were taken to secure the classified information and/or limit the damage before a report was made and an administrative inquiry was completed. When and by whom were they taken? (Inventories of classified material, changing of combinations, etc.)

E. Disciplinary Actions Related to Security Violations

The most frequent type of security violation that occurs is unintentional and caused by human error. Continuous security awareness is our most effective means of minimizing these types of violations. Following are some common human errors noted throughout industry:

1. A safe or cabinet approved to store classified material is left unlocked and unattended. (Always check to see that the container is locked prior to leaving the area).

2. Classified material is hurriedly placed in a desk drawer when someone not authorized to see it approaches, and then inadvertently, left there overnight or longer. (Either keep the material with you or return it to the approved storage container).

3. Classified information is inadvertently entered into a computer system not approved for classified processing, or into an unclassified document. (Be thoroughly familiar with the classification of the information you are working with).

4. Information believed to be unclassified is downloaded from a classified computer system onto a diskette, tape or paper. It is not reviewed properly by the person responsible and is later found to contain classified information. Prior to the classified contents being discovered, the media has been handled as unclassified and has been accessed by unauthorized persons, and/or sent out of the facility as unclassified material. (Follow the procedures required by the Automated Information System (AIS) Security Plan).

5. Classified material being hand-carried to or from another location is left unattended in a vehicle, hotel room, or stored in a hotel or private residence. (Never transmit classified material by hand-carrying unless absolutely necessary).

Disciplinary action taken by this facility will be based upon a review of each case’s own merits. The seriousness of the violation will be determined by whether a compromise, suspected compromise, or loss of classified information has occurred, or if it was only administrative in nature.

The company’s disciplinary action may be any one of the following depending upon the above factors:

1.

2.

3.

# SECTION 3

## INDIVIDUAL RESPONSIBILITIES

A. Safeguarding Classified Information

1. Each cleared employee of this facility is required to safeguard classified information entrusted to his or her care. Specific containers have been approved for the storage of classified material in this facility. Only these designated containers may be used to store classified material. When classified material has been removed from its container it must remain under the direct supervision of an authorized appropriately cleared employee at all times.

2. Employees should choose private office space or other approved areas to perform classified work, where access by unauthorized personnel can easily be precluded. Should an unauthorized person enter your work area while classified work is in progress, the classified material should be covered or turned over. Never place classified material inside a desk or other unapproved container for any length of time.

3. Combinations to classified containers are classified to the highest level of information authorized for storage in the container, therefore, if a record of the combination is made it must be stored inside a classified container.

4. Do not provide classified information to another individual unless that person has the proper level security clearance, and the need-to-know for the information involved. Physically check the person’s identity by personally reviewing an official form of photo identification such as a driver’s license, passport, or credentials. Compare the photo against the individual’s appearance. Compare identifying information against employee records or against a visit authorization letter on file in the security office. Before releasing classified information to anyone or before allowing unescorted access to a closed or restricted area, identify the most restrictive classification involved and compare it to the person’s clearance level. Remember that there are access limitations associated with contractor-granted Confidential, interim and Limited Access Authorization (LAA) clearances. If the information to be accessed requires a special briefing, i.e., NATO, COMSEC, CNWDI, you must also verify that the person has received the proper briefing.

5. Do not attempt to “talk around” classified information over the telephone, unless you are using an authorized secure telephone line.

6. Do not remove classified material from this facility without prior approval from the Facility Security Officer or his/her designee.

7. Do not enter classified information into any automated information system, to include computers, test equipment, etc., without the prior approval of the Facility Security Officer.

B. Reporting Information

Each cleared employee of this company shall report to the Facility Security Officer any of the following:

1. Espionage—Information concerning existing or threatened espionage, sabotage or subversive activities.

2. Compromise—The loss, compromise or suspected compromise of classified information whether inside or outside of the company.

3. Security Violation—Any failure to comply with a requirement of this SPP or of the NISPOM.

4. Suspicious Contacts—Any efforts by an individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. In addition, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country shall be reported.

5. If you: change your name; change your citizenship; change your marital status (marriage and divorce must be reported by employees cleared TOP SECRET or having access to Sensitive Compartmented Information (SCI); complete work on a classified contract and are no longer having access on other classified contracts; begin work on a foreign contract (classified or unclassified); are assigned to work outside of the United States.

6. Any cleared employee who becomes a Representative of a Foreign Interest (RFI) or whose status as an RFI has materially changed. An RFI refers to a citizen or national of the US or immigrant alien who, in his/her individual capacity or on behalf of a corporation (whether as a corporate officer or official or as a corporate employee who is personally involved with the foreign entity), is acting as a representative, official, agent, or employee of a foreign government, firm, corporation, or person.

7. Adverse Information—Any information coming to your attention concerning another cleared employee or an employee in process for a security clearance that could be an indication that such access may not be in the best interest of national security, or that a person’s ability to Safeguard classified information may be impaired. Some examples of adverse information are: illegal activities, excessive use of intoxicants, treatment for mental or emotional disorders, recurring financial difficulties, or unusual affluence.

C. Responsibilities of Supervisors and Managers

- Ensure that a current copy of the Security SPP is available for cleared employees within their work area.

- Make employees available for scheduled security briefings.

- Provide adequate justification for any personnel security clearances requested.

- Report to the FSO the receipt of any new classified contract, bid, etc. (U.S. and foreign).

- Report to the FSO the need for a larger storage area for bulky or large classified material.

- Report to the FSO the need to perform classified work on computer systems not yet accredited for classified processing.

- Report changed contractual requirements that may affect the company’s security requirements.

- Report the completion of work on a classified contract.

*All of the above responsibilities are in addition to the individual responsibilities of employees.*

# SECTION 4

## THE FACILITY SECURITY OFFICER

Our FSO is:

Our Assistant to the FSO is:

A. FSO’s Responsibilities

1. The FSO for this company is responsible for administering the security program and for performing the following functions:

2. Receives, prepares and submits reports. Reports concerning changes in the company, security violations, and classified contractual security needs are submitted to the Cognizant Security Office. Reports concerning individuals’ security clearances are submitted to the Defense Industrial Security Clearance Office (DISCO) in Columbus, Ohio. Some reports may be submitted to the local office of the FBI.

3. Maintains all facility clearance records, to include the “Letter of Notification of a Facility Security Clearance,” DD Form 441 (or 441-1)”Department of Defense Security Agreement,” and DD Form 441s, “Certificate Pertaining to Foreign Interests.”

4. Maintains all personnel security clearance records, to include DISCO Form 560, “Letter of Consent,” a record of Security Briefing for all cleared employees, and DISCO Form 562, “Personnel Security Clearance Change Notification,” where applicable.

5. Maintains the NISPOM and any changes to the NISPOM upon notification.

6. Briefs all cleared employees on their responsibilities for safeguarding classified information and ensures the SF-312, “Classified Information Nondisclosure Agreement” is properly executed.

7. Processes requests for Confidential, Secret or Top Secret government security clearances.

8. Conducts a self-inspection at intervals consistent with risk management principles and reviews the company security program on a continuous basis.

9. Serves as the principal point of contact for representatives of DSS.

*Our FSO will submit the following reports to DISCO:* (paragraphs 1-302a through 1-302g, NISPOM)

* Adverse Information

- Suspicious Contacts

- Change in Cleared Employee Status

- Representative of a Foreign Interest

- Citizenship by Naturalization

- Employees Desiring Not to Perform on Classified Work

- SF 312

*The following reports will be submitted to the CSA:* (paragraphs 1-302h through 1-302o, NISPOM)

- Changed Conditions Affecting the FCL

- Change in Storage Capability

- Inability to Safeguard Classified Material

- Security Equipment Vulnerabilities

- Unauthorized Receipt of Classified Material

- Employee Information in Compromise Cases

- Disposition of Classified Material Terminated from Accountability

- Foreign Classified Contracts

# SECTION 5

## PERSONNEL SECURITY CLEARANCES

A. Request for a Security Clearance

Employees will be processed for a personnel security clearance (PCL) only when a determination has been made that access is necessary for performance on a classified contract. The employee must have a “need-to-know” for the information. A clearance is valid for access on a need-to-know basis to classified information at the same or lower level of classification as the level of the clearance granted. Clearances are granted either at the Confidential, Secret or Top Secret level. All personnel security clearances are granted by the Defense Industrial Security Clearance Office (DISCO) in Columbus, Ohio.

DISCO will provide written notice when an employee’s PCL has been granted, denied, suspended, or revoked. Our facility must immediately deny access to classified information to any employee when notified of a denial, revocation or suspension. DISCO will provide written notice to us when processing action for PCL eligibility has been discontinued. Our personnel may be subject to a reinvestigation program by DSS.

B. Application for a Security Clearance

A Single Scope Background Investigation (SSBI) is required for Top Secret, Q and Sensitive Compartment Information (SCI) access. Application must be made on an SF Form 86 for DoD, DoE and NRC contractors. A National Agency Check and Credit Check (NACC) are required for Secret, L and Confidential access. Application must be made on an SF Form 86 for DoD, DoE and NRC contractors. Normally, application for a security clearance shall be made electronically using the Electronic Personnel Security Questionnaire Program or EPSQ.

A revalidation of a security clearance is a reinstatement of a clearance that has been previously terminated. A new investigation is not conducted at this time. A periodic reinvestigation or PR is a new investigation conducted on a person currently holding a security clearance.

Reviewing the SF 86

1. Forms must be typed or handwritten in black ink only.

2. All questions must be answered, none or N/A where applicable.

3. For item #8 (citizenship):

*If born abroad, you must provide the following Naturalization Information:*

- Certificate Number

- Date of Naturalization

- Place where Naturalization occurred

- Court where Naturalization occurred

- Alien Registration number, if not naturalized

- If the application is for a Confidential or Secret clearance this information is required only for the subject.

- This information is required for Top Secret Periodic Reinvestigations also.

4. For item #9 (residence):

- All residences for the last 7 years are required, complete with street number and name, city, state, and the zip code.

- For all Military residences list every address individually; be sure to indicate the country if out of U.S.

- Leave no gaps in dates.

5. For item #11 (employment):

- List all employment for last 7 years, with complete addresses to include the zip codes.

- Leave no lapses in employment; if self- or unemployed, provide references who can verify these dates.

- For military service, do not list one time period to cover entire military service; list each individual duty station separately with complete addresses, to include zip codes and country if other than U.S.

- List all Federal Civil Service, even if out of 7 year scope, with complete addresses.

- List the company with whom you will be holding a clearance as your most current employment, even if you are not physically working there on a daily basis. (This will let the investigator know where to go for the subject interview).

6. For item #14 (family and associates):

- List all information completely, and give naturalization information for any relative that is naturalized and living IN the U.S. If relative was born, lives and is a citizen of another country, naturalization information is not required. If the person is a U.S. citizen and residing in another country, give naturalization information.

- This information is also required for Periodic Reinvestigations for Top Secret level only.

7. For item #17 and #18 (foreign activities and travel):

- List all countries, dates, and purpose of visits.

- Do not copy passports.

- Currently we require this information to make a Foreign Representative determination: Percentage of ownership; citizenship of those owners; what is nature of business for the U.S. facility and the foreign entity(s); subject’s specific duties with the foreign entity(s).

8. For item #20:

- The DD Forms 398 and 398-2 contain no question like this.

9. For item #21 (medical):

- List nature of illness, type of treatment, beginning and ending dates of all treatment, diagnosis, and name and complete address of doctor and /or facility where treatment has taken place. Note that the SF 86 only asks for dates and the name and address of the doctor/therapist.

10. For item #22 (your employment record):

- The DD Form 398 and 398-2 do not ask for this information.

11. For item #23 (arrest record):

- Don’t list penal codes as type of offense; list actual offense arrested for.

12. For item #24 (illegal drugs):

- Provide names of drugs used, dates to and from, frequency of use, and future intent of use.

13. For item #27 (financial record):

- Provide beginning and ending dates, amount of indebtedness, city, state, name and location of organization involved.

14. For item #29 (public record civil court actions):

- The DD Form 398 and 398-2 has no question like this.

The application will be completed jointly by the employee and the FSO or designee. Page 5 of the DD Form 398 and 398-2 and part 2 of the SF Form 86 may be completed in private and returned to the FSO in a sealed envelope. The contents of the sealed envelope may not be viewed by anyone else but the employee. The application along with sealed envelope will be sent to DISCO for processing. Complete and accurate information provided by the employee will enable quicker processing of the security clearance.

The Electronic Personnel Security Questionnaire or EPSQ Program allows contractors to use software provided by DSS, to transmit an application for a security clearance electronically to DISCO. This is the preferred method for applying for a clearance because it virtually eliminates omissions and errors on the application and significantly shortens processing time. Using the EPSQ Program requires the employee to fill out answers to the application questions in print. The form will then be provided to the FSO or designee, who will enter the information into a computer system to be electronically transmitted to DISCO.

Proof of Citizenship

Each applicant for a security clearance who claims U.S. citizenship must produce evidence of citizenship. For individuals born in the United States, a birth certificate is the primary and preferred means of citizenship verification. Acceptable certificates must show that the birth record was filed shortly after birth and it must be certified with the registrar’s signature. It must bear the raised, impressed, or multicolored seal of the registrar’s office. The only exception is if a state or other jurisdiction does not issue such seals as a matter of policy. Uncertified copies of birth certificates are not acceptable.

For individuals who claim citizenship by naturalization, a certificate of naturalization is acceptable proof of citizenship. If citizenship was acquired by birth abroad to a U.S. citizen parent or parents, the following are acceptable evidence:

* a Certificate of Citizenship issued by the Immigration and
* Naturalization Service, or
* a Report of Birth Abroad of a Citizen of the United States of
* America (Form FS-240), or
* a Certificate of Birth (Form FS-545 or DS-1350).
* a current or expired passport
* Record of Military Processing-Armed Forces of the United States (DD Form 1966) if it reflects U.S. citizenship.

Fingerprints

Our facility must ensure that the taking of the applicant’s fingerprints is witnessed to ensure they are, in fact, the same as the person being processed for the clearance.

The fingerprint cards along with the application will be submitted to DISCO. When a Letter of Consent for the individual processed is received and after the employee has executed the Classified Information Nondisclosure Agreement (Form SF 312) and has received an initial security briefing he or she is then eligible for access to classified information at the prescribed level.

C. Processing a Security Clearance

Federal agencies that grant security clearances to contractor employees are responsible for determining whether the employees have been previously cleared or investigated by the Federal Government. Any previously granted PCL that is based upon a current investigation of a scope that meets or exceeds that necessary for the clearance required, shall provide the basis for issuance of a new clearance without further investigation or adjudication unless significant derogatory information that was not previously adjudicated becomes known to the granting agency.

For Multiple Facility Organizations (MFOs), two options are available: (a) All Letters of Consent may be issued to the Home Office of the MFO, or (b) Letters of Consent may be issued to individual cleared facilities within the MFO, to a designated Principal Management Facility within an MFO or a combination thereof. PCLs will be issued to the Home Office unless an alternative arrangement is approved by the Cognizant Security Office.

Interim PCLs

Applicants for Top Secret, Secret and Confidential PCLs may be routinely granted interim PCLs at the Secret and Confidential level, as appropriate, provided there is no evidence of adverse information of material significance. Applications for Interim Top Secret PCLs must be submitted to the pertinent Government Contracting Activity (GCA).

An interim Secret or Confidential PCL is valid for access to classified information at the level of the interim PCL granted, except for Sensitive Compartmented Information, Restricted Data, COMSEC Information, SAP, and NATO information. An interim Top Secret PCL is valid for access to Top Secret information and Restricted Data, NATO information and COMSEC information at the Secret and Confidential level.

Reinstatement of a PCL

A security clearance can be reinstated at our facility or at another cleared facility provided (a) No more than 24 months has lapsed since the date of termination of the clearance; (b) There is no known adverse information;(c) The most recent investigation must not exceed 5 years (TS, Q) or 10 years (Secret, L); and (d) Must meet or exceed the scope of the investigation required for the level of clearance that is to be reinstated or granted. The clearance can be reinstated at the same or lower level by submission of the DISCO Form 562. Access may not be granted until the Letter of Consent is received from DISCO.

Employees possessing a valid PCL (at the appropriate level) from another Government agency shall not be required to complete a DD Form 398 or 398-2. A DISCO Form 562 will be submitted to DISCO, which will verify the existence of the PCL. A Letter of Consent will then be issued by DISCO if there is a current PCL at the required level that can be verified.

The DISCO Form 562 can be sent via FAX to DISCO using the following number: (614) 692-1410.

The DISCO Form 562 is in the process of being revised. In the interim the 562 will be completed using the following guidelines for requests for conversions, revalidations, reinstatements and concurrent clearances:

|  |  |
| --- | --- |
| Item 1, O “Other” | Type of action requested |
| Item 4 | Enter current requester information |
| Item 11 | Enter previous clearance information |
| Item 14 | Enter level of clearance requested |
| Items 5, 6, 7, 8, 9, 10, 12, 13, and 15 | Self-explanatory |

Concurrent PCL’s

A concurrent PCL can be issued if our facility hires an employee or engages a consultant who has a current PCL, where a Letter of Consent for the individual has been issued to another facility. We cannot provide the individual access to classified information until this facility receives a Letter of Consent.

Converting PCL’s to Industrial Clearances

PCLs granted by government agencies may be converted to industrial clearances when: (a) A determination can be made that the investigation meets standards prescribed for such clearances; (b) No more than 24 months has lapsed since the date of termination of the clearance; and, (c) No evidence of adverse information exists since the last investigation. Normally a DISCO Form 562 will be submitted when requesting conversion of a PCL. Access may not be granted until receipt of a Letter of Consent.

D. Termination of a Security Clearance

When an employee no longer requires access to classified information and a need for access in the future can be reasonably foreclosed, the individual’s clearance will be administratively terminated. In addition, clearances must be terminated upon the termination of an employee’s employment with the facility. Should either one of these events occur, the employee will be advised that the action is being taken. The clearance is terminated by submission of a DISCO Form 562 to DISCO.

The SF 312 Form may be sent to DISCO upon termination by FAX.

# SECTION 6

## SECURITY EDUCATION

Working with classified information makes each of us a potential target for hostile intelligence interests. It’s everyone’s responsibility to be aware that there really are agents who seek to obtain bits and pieces of defense-related information. Each of us must ensure classified information is not compromised. Hostile intelligence agents also target unclassified but sensitive proprietary information which can be valuable to the economic and defense interests of foreign governments. We must also ensure company proprietary information is safeguarded and access to it also strictly limited.

A. Initial Security Briefing

Prior to being granted access to classified information, all employees must receive an initial security briefing that includes the following:

1. A Threat Awareness Briefing.

2. A Defensive Security Briefing.

3. An overview of the security classification system.

4. Employee reporting obligations and requirements.

5. Security procedures and duties applicable to the employee’s job.

6. Execution of the SF 312, Classified Information Nondisclosure Agreement.

All employees shall be made aware that Classified Information is information requiring protection from disclosure to unauthorized persons in the interest of national security. There are three levels of classification:

1. **TOP SECRET** - the designation applied to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

2. **SECRET** - the designation applied to information or material the unauthorized disclosure of national security.

3. **CONFIDENTIAL** - the designation applied to information or material the unauthorized disclosure of which could be reasonably expected to cause damage to the national security.

Classified material may only be stored in designated containers or controlled areas. When not properly stored, it must be in the possession of a cleared employee at all times. No one may release classified information to another individual without first verifying the recipient’s security clearance level. This is accomplished by contacting the Facility Security Officer or designee. No employee is permitted to remove classified material from the premises of this facility unless, specifically authorized to do so by the FSO.

B. Refresher Security Briefing

Periodically, our cleared employees will receive refresher briefings. Scheduled refresher briefings are important to you as an employee because they may include changed security requirements that may affect you, and they serve as a reminder of important requirements that relate directly to the work you are presently involved with.

C. Threat Awareness Briefing

National Security Begins with You …

We live in a world of rapid change. In recent years the FBI has seen marked shifts in the area of international relations. Reflecting these shifts, the Attorney General has rearticulated the FBI’s Foreign Counterintelligence mission in a strategy known as the National Security Threat List (NSTL). The NSTL combines two elements. First, it includes national security issues that the FBI has concluded need to be addressed no matter where the threat comes from or what country is involved. Second, it includes a classified list of foreign powers that pose a strategic intelligence threat to U.S. security interests.

Issue Threats

* Proliferation of special weapons of mass destruction to include chemical, biological, nuclear, and delivery systems of those weapons of mass destruction.
* Collection of information relating to defense establishments and related activities of national preparedness.
* U.S. critical technologies as identified by the National Critical Technologies Panel.
* Targeting of U.S. intelligence and foreign affairs information and U.S. Government officials.
* Collection of U.S. industrial proprietary economic information and technology, the loss of which would undermine the U.S. strategic industrial position.
* Clandestine foreign intelligence activity in the United States.
* Perception management and active measures activities.

National Critical Technologies

* Materials
* materials synthesis and processing
* electronic and photonic materials
* ceramics
* composites
* high-performance metals and alloys
* Manufacturing
* flexible computer-integrated manufacturing
* intelligence processing equipment
* micro and nanofabrication
* systems management technologies

Information and Communications

* software
* micro and optoelectronics
* high-performance computing and networking
* high-definition imaging and displays
* sensors and signal processing
* data storage and peripherals
* computer simulation and modeling

Biotechnology and Life Sciences

* applied molecular biology
* medical technology

Aeronautics and Surface Transportation

* aeronautics
* surface transportation technologies

Energy and Environment

* energy technologies
* pollution minimization, remediation, and waste management

National Security Begins with You

You may be the target of foreign intelligence activity if you or your company is associated with one or more of the critical technologies. Foreign powers may also seek to collect U.S. industrial proprietary economic information and technology, the loss of which would undermine the U.S. strategic industrial position. Foreign intelligence collectors do, today, target corporate marketing information in support of their Nation’s firms. Overseas travel, foreign contact, and joint ventures may further increase your company’s exposure to the efforts of foreign intelligence collectors. If you suspect foreign intelligence activity, or have questions concerning the National Security Threat List strategy, contact your local FBI office.

D. Defensive Security Briefing

Although the Designated Country list has been rescinded by the Defense Security Service, U.S. Technology is still targeted by foreign nations. It is far less expensive to use existing technology than it is to develop new technology. This technology threat pertains to classified, sensitive protected company proprietary, and other unclassified protected information.

As a traveler, you are more vulnerable because you may be unfamiliar with the customs, people, language, topography, laws and judicial system of the country. You become more dependent upon strangers. This is an attractive situation for the foreign agent. The same opportunities exist in both “friendly” and “unfriendly” countries.

Be suspicious. The operative of a foreign intelligence service need not be a foreigner, or the occasion where contact is made need not be in anyway extraordinary. Be especially aware the following circumstances provide perfect opportunities for foreign intelligence agents to contact you. Be alert to overly friendly or helpful strangers. Do not fall into a compromising situation where outside help may be needed or threats of blackmail could surface. Examples of behavior which have led to problems for other U.S. travelers are:

* Involvement in illicit currency trade
* Poor judgment in alcohol consumption
* Minor traffic violations
* Gambling
* Any immoral conduct
* Viewing political demonstrations or parades

Be a smart traveler. Consider the following actions that you can take when traveling outside of the U. S.:

(1) Carry personal identification and any special medical information with you at all times.

(2) Maintain a low profile when in foreign countries on business; don’t advertise your presence and sensitive knowledge you may possess unnecessarily.

(3) Never leave important papers regarding technology or personal papers which could cause embarrassment to you unattended in a hotel room. Anything left unaccompanied is susceptible to being copied or stolen.

(4) Never hold sensitive or classified discussions in your hotel room or in a room provided for you by the host country.

(5) When filling out landing cards on aircraft or registering in hotels give only that information necessary to accomplish the task. There is no reason to say you are the chief engineer on a project or a company president. Likewise there is no need to indicate that you are visiting the country to display your classified items at the exhibit.

(6) Beware of individuals who demonstrate unusual interest in your visit and your company.

(7) Don’t advertise that you are a US Government contractor. Likewise, clean out your billfold, purse and luggage prior to a trip; don’t carry excess papers that might identify you with a classified project or sensitive technology.

(8) Do not leave your wallet or purse unattended.

(9) Keep a low profile and avoid giving an impression of wealth.

(10) Carry international traveler’s checks and always exchange currency at reputable currency exchanges (it is illegal to do otherwise in some countries).

(11) Drive carefully (you may want to apply for an international driver’s license if you plan on traveling extensively by car).

(12) Observe local laws and customs. For example, in Turkey, Taiwan and Spain, individuals are prohibited from making derogatory comments about the government or its leaders. In other countries it is unlawful to use insulting language or abusive gestures toward another person while driving. Remember you are representing the United States while abroad. Avoid political discussions, and remember you may encounter anti-American sentiments. Be patient rather than critical of local customs. Be a smart traveler.

(13) Remember, classified material, whether U.S. or belonging to a foreign government, may not be stored in a hotel room and may only be transmitted to or from the United States using established government to government channels.

If you have something to report, please notify security on the first day you return to work. If in doubt, please visit your security office representative to discuss even the most minor incidents. Remember:

* Report any attempt by a foreign national or stranger to establish a continuing association, or arrange future meetings or correspondence.
* Report any contact with anyone whom you suspect may be attempting to gather classified or company proprietary information.
* Maintain a high level of personal standards and conduct. Keep in mind you are a foreign guest and a representative of the United States.

E. Debriefings

All employees must be provided a debriefing at the time of termination of employment or when an employee’s clearance is terminated, suspended or revoked. The debriefing shall remind the individual that they continue to be obligated to protect classified information to which they had access while cleared under the laws of the United States, even after termination of the security clearance. The individual shall again review the appropriate portions of Title 18 and Title 50, United States Code and the provisions of the Intelligence Identities Protection Act of 1982.

For those SF 312 Forms executed after July 31, 1995, the SF 312 shall be forwarded to DISCO. For those executed prior to that date, we shall retain the SF 312 until advised by DSS to forward them to DISCO.

# SECTION 7

## CLASSIFIED VISITS

At times during the performance of a classified contract, or during the pre-award phase or bid negotiations for a classified contract, cleared employees may require access to classified information at another contractor’s facility or at a government activity. Employees of other cleared contractor facilities and government activities may require access to classified information in the possession of our facility. Through a process of notification and approval of visits, classified access to visitors is permitted. The Visit Authorization Letter or VAL is the vehicle used for notification of incoming and outgoing classified visits.

The number of classified visits shall be held to a minimum. There must be a determination in each case that the visit cannot be achieved without access to, or disclosure of, classified information. All classified visits require advance notification to and approval of, the organization being visited.

Visits by Federal Government Representatives, when acting in their official capacities as inspectors, investigators, or auditors, may visit our facility without furnishing advance notification, provided these representatives present appropriate government credentials upon arrival. You may contact the Facility Security Officer to confirm the identity of a Government representative when in doubt.

A. Incoming Visits

All incoming classified visits must be approved in advance of the visit by the Facility Security Officer. The FSO or his/her designee is responsible for determining that the requesting contractor has been granted an appropriate facility clearance, based either upon an existing contractual relationship involving classified information of the same or higher category, or by verification from the Defense Security Service/Central Verification Activity (DSS/CVA) at (410)631-0690. A Visit Authorization Letter from the visitor’s organization must have been received and requires the following information:

1. Contractor’s name, address, and telephone number, assigned CAGE Code, if applicable, and certification of the level of the facility security clearance.

2. Name, date and place of birth, and citizenship of the employee intending to visit.

3. Certification of the proposed visitor’s personnel clearance and any special access authorizations required for the visit.

4. Name of the person(s) to be visited.

5. Purpose and sufficient justification for the visit to allow for a determination of the necessity of the visit.

6. Date or period during which the VAL is to be valid.

For each classified visit to our company the following information must be recorded in our visitor log book:

(a) The visitor’s name

(b) The name of the activity represented

(c) The date of the visit

The responsibility for determining need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit. Prior to the disclosure of classified information to a visitor positive identification of the person must be made.

When there is no classified contractual relationship between the parties, classified information may not be disclosed without the prior approval of the Government agency that has jurisdiction over the information.

B. Outgoing Visits

Our facility has a VAL which shall be used by all cleared employees required to make classified visits to another facility. A sample of our VAL is included in Section 18 of the SPP.

A VAL should not be sent unless there is a valid need for classified access during the visit.

When the clearance status of an employee changes, security must determine if there are any outstanding VAL’s for the individual and cancel them if necessary.

C. Meetings

Employees must contact the FSO prior to hosting a classified meeting. A classified meeting refers to a conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which classified information is disclosed. Should our facility desire to host a classified meeting, we must first obtain authorization from a Government Agency that has agreed to assume security jurisdiction. The Government Agency must approve security arrangements, announcements, attendees, and the location of the meeting. The Government Agency may choose to delegate some of responsibilities for security arrangements to our facility.

If our company wishes to disclose classified information at a meeting, we must first obtain prior written authorization for each proposed disclosure of classified information from the Government Agency having jurisdiction over the classified information involved.

# SECTION 8

## STORAGE OF CLASSIFIED MATERIAL

In our facility classified material must be stored in a security container that has been previously approved by DSS. Chapter 5, Section 3 of the NISPOM outlines the specific storage requirements for Confidential, Secret and Top Secret material in the custody of contractors. A safe approved by the General Services Administration (GSA) is normally used for the storage of classified material. For Confidential and Secret material, no supplemental protection is required if it is being stored in a GSA-approved safe.

In some instances a room or area may have to be approved for classified material storage due to the size or nature of the material involved. Such an area is called a closed area, and must be approved by DSS and the FSO. If Secret material is to be stored in such an area, supplemental protection will be required. Supplemental protection is generally provided by use of an approved alarm system, or if cleared security guards have been used prior to January 1995 they may continue to be used for additional closed areas.

When it is necessary to control access to classified information in an open area during working hours, a Restricted Area may be established. A Restricted Area will normally become necessary when it is impractical or impossible to protect classified material because of its size, quantity or other unusual characteristic. The Restricted Area must have a clearly defined perimeter, but physical barriers are not required. Personnel within the area are responsible for challenging all persons who may lack appropriate access authority. All classified material must be secured during non-working hours in approved containers/areas.

Should a container or closed area require any physical repair or modification you must obtain approval and instructions from the FSO beforehand. The FSO will maintain a list of all approved containers and closed areas.

A record of the names of persons having knowledge of classified combinations must be maintained by our company. Only a minimum number of authorized persons shall be given combinations to classified storage containers and areas. The combinations will be safeguarded in accordance with the highest classification of the material authorized for storage. When an employee having knowledge of a classified combination terminates employment, or no longer requires the combination, or if there is a suspected compromise of the combination, it must be immediately changed by an authorized, cleared employee. Combinations may only be stored in an employee’s memory or in an approved classified container.

Removal of classified material by company employees for use or storage at a private residence is not authorized.

Our company may, at times, conduct perimeter control inspections during which employees’ hand-carried items may be inspected by or under the direction of the FSO. Such inspections are necessary to assist us in the detection of any unauthorized introduction or removal of classified material. All persons who enter or exit our facility are subject to an inspection of their personal effects.

At the close of each working day employees are responsible for ensuring that all classified material has been secured. All security containers and/or closed areas in your respective work areas must be checked to verify they are properly locked. Work areas must be inspected to ensure no classified material has been left out. Whenever possible, a second cleared employee is required to double check that classified material has been secured.

A. Automated Information Systems

In the NISPOM, computer systems are called Automated Information Systems or AIS. An AIS must be approved by DSS and the FSO before you may enter classified information into it. Protection of the entire AIS must include features of the AIS, administrative, operational, physical and personnel controls. An AIS approved to process classified information requires an Information Systems Security Representative or ISSR and an AIS Security Plan.

The ISSR must be an appropriately cleared employee, not necessarily the FSO, who will be responsible for the following:

* Maintain liaison with the Cognizant Security Office.
* Implement and administer the company’s AIS Security Policy.
* Ensure the preparation of an AIS Security Plan.
* Ensure the establishment and maintenance of security safeguards and access controls.
* Ensure that users have the security clearance, special access authorizations, and need-to-know for the information that they can access.
* Ensure that all AIS security related documentation is current.
* Advise the FSO and CSO of any abnormal event that affects the security of the AIS.
* Ensure that secure maintenance procedures are followed.
* Ensure that security audit records are maintained, accessible, and reviewed and analyzed according to the schedule required by the AIS Security Plan.
* Assist in the development and implementation of an ongoing AIS security education program.
* Perform threat based, aperiodic inspections pursuant to the AIS SP.
* Approve and document the movement of AIS equipment.
* Approve the release of sanitized equipment and components in accordance with the sanitization matrix on page 8-3-5 of the NISPOM.

Additional responsibilities may be necessary depending upon the complexity of the AIS approved.

For all other requirements concerning classified AIS processing see the AIS Security Plan.

# SECTION 9

## CONTROL OF CLASSIFIED MATERIAL

Our company is required to establish an information management system and must control classified information in our possession. Classified information may be retained only in furtherance of a lawful and authorized U.S. Government purpose. The U.S. Government reserves the right to retrieve its classified material or to direct us to dispose of it using approved methods. The information management system we employ must be capable of facilitating such retrieval and disposition in a reasonable period of time.

The FSO must maintain a record that reflects: (a) The date of the material; (b) The date of receipt or dispatch of the material; © The classification; (d) An unclassified description of the material; and (e) The identity of the activity from which the material was received or to which the material was dispatched.

*(See Section 15 for Top Secret Control Requirements)*

All classified material shall be delivered unopened to personnel designated by this company to receive it. All employees who handle U.S. Registered, U.S. Certified or U.S. Express Mail must be appropriately cleared.

Anyone receiving Federal Express mail should look closely for any markings indicating that the material is classified. If the inner package has classification markings, deliver the package to the FSO immediately.

Disclosure of Classified Material

Prior to disclosing classified material to another individual it is each employee’s responsibility to verify through the office of the Facility Security Officer the security clearance and need-to-know of the intended recipient. In addition, a decision must be made beforehand, that disclosure of the classified information is necessary in the performance of a classified contract, bid, proposal or project.

Department of Defense classified information may be shared between DoD classified efforts. Release of information to another User Agency requires the permission of the User Agency owning the information.

# SECTION 10

## TRANSMISSION OF CLASSIFIED MATERIAL

The FSO or designee shall be responsible for approving of all outgoing transmission of classified material, and for the preparation of the material for transmission. The classified material and receipt will be packaged in opaque inner and outer containers or wrapping. The inner container or wrapping will be addressed, return addressed and marked on all sides with the appropriate classification level and will contain the receipt. The outer container or wrapping will reflect the classified mailing address and return address only. The FSO must obtain the proper classified mailing address of the activity to receive the material. The receipt that will be used for classified transmissions is shown in Section 19.

A. Transmission of Classified Material Outside the Facility

Secret material may be transmitted by one of the following methods within and directly between the U.S., Puerto Rico, or a U.S. possession or trust territory:

(1) By the methods established for Top Secret (see Section 15).

(2) U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail. Note: The “Waiver of Signature and Indemnity” block on the U.S. Postal Service Express Mail Label 11-B may not be executed and the use of external (street side) express mail collection boxes is prohibited.

(3) A cleared Commercial Carrier.

(4) A cleared commercial messenger service engaged in local/intra-city area delivery (same day delivery only) of classified material.

(5) A commercial delivery company approved by the CSA, that provides nation- wide, overnight service with computer tracking and reporting features.

Confidential material may be transmitted by the methods established for Secret material or by U.S. Postal Service Certified Mail.

Any transmission of classified material to another country, whether to a foreign government or a U.S. government activity, requires special handling and must be coordinated with DSS or another Government Activity.

B. Courier Procedures and Courier Briefing

Anyone who hand-carries classified material from our facility must satisfy all the following requirements for couriers. This includes anyone who picks up or delivers U.S. Registered, Certified, or Express Mail as well as employees otherwise carrying packages of classified material outside our facility. Couriers must be:

1. Cleared to the appropriate level required for the most restrictive classification of the material to be hand-carried.

2. Designated in writing (utilizing the appropriate company letterhead) to perform courier duties by the FSO.

3. Briefed in their courier responsibilities by the FSO when they are designated.

**The Courier Briefing**

You are hereby designated a courier for the transmission of Department of Defense Classified material. In this capacity, it is mandatory that you fulfill the following requirements:

1. Ensure that the transmittal is necessary in connection with a prospective or current classified procurement or an approved classified meeting and that the FSO or designee has authorized the hand-carry.

2. Ensure that time limitations prevent transmitting the material by the appropriate U.S. mail service or approved commercial carrier.

3. Ensure that only that classified material essential for the purpose of the visit or hand-carry is being carried.

4. The material must be prepared and packaged in accordance with our security SPP and the NISPOM. One copy of the inventory of the material being transmitted will be carried on your person and a second copy will be left with the security office. You will not accept custody or release of classified material without the exchange of receipts.

5. While traveling, you are required to proceed directly to the facility designated to receive the material. You are personally responsible for the protection and proper delivery of the classified material entrusted to your care. You must conduct yourself in such a manner that the security of the classified material in your care will not be prejudiced or compromised through carelessness or lack of vigilance. The fact that you are transporting classified material shall not be divulged to unauthorized persons. Classified material shall not be read or displayed in any manner in public conveyances or places.

6. Intoxicants or drugs (which may impair an individual’s judgment or physical capabilities) may not be used while having custody of classified material.

7. The classified material must be continuously in your possession while traveling and shall not be left in such places as vehicles (locked or unlocked), hotel rooms, hotel safes, train compartments, etc. Classified material being hand-carried must be kept under your constant surveillance. Therefore, you may not sleep while such material is in your possession.

8. During any stopover, the classified material will remain under your constant surveillance unless arrangements have been made in advance of your departure for storage of the hand-carried classified material at a U.S. Government installation or a cleared contractor facility.

9. In the event of an emergency, immediately notify our Security Officer. If a problem arises and our company cannot assist you, contact the nearest U.S. Government activity or cleared contractor facility for assistance.

I have read and fully understand my courier responsibilities as described above.

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

Courier’s Signature Date

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

Witness Signature

# SECTION 11

## CLASSIFICATION AND ORIGINATION OF CLASSIFIED MATERIAL

Information is classified pursuant to Executive Order 12356 by an original classification authority and is designated and marked as TOP SECRET, SECRET, or CONFIDENTIAL. No other designations may be used to identify classified national security information. Sensitive unclassified information may be identified by other caveats or markings, such as For Official Use Only (FOUO) and Naval Nuclear Propulsion Information (NNPI). The safeguarding of such unclassified Government information is covered by other directives, instructions and regulations.

An original classification decision at any level can be made only by a U.S. Government official who has been delegated the authority in writing. Original classification decisions may require a security classification guide be issued for use in making derivative classification decisions. Contractors make derivative classification decisions based on the guidance provided by the Contract Security Classification Specification (DD Form 254) that is issued with each classified contract.

A. Origination of Classified Material

Employees authorized to perform derivative classification actions must have adequate training and the proper classification guides and/or guidance necessary to accomplish these important actions.

The following guidelines must also be met:

1. The manager or supervisor at the operational level where material is being produced or assembled shall determine the necessity, currency, and accuracy of the classification applied to that material.

2. The manager or supervisor whose approval is required before the material is transmitted outside the facility shall determine the necessity, currency, and accuracy of the security classification applied to that material.

3. Employees who copy or extract classified information from another document, or who reproduce or translate an entire document, shall be responsible for (a) Marking the new document or copy with the same classification markings as applied to the information or document from which the new document or copy was prepared and (b) Challenging the classification if there is reason to believe the information is classified unnecessarily or improperly.

4. Whenever our facility develops an unsolicited proposal, or originates information not in the performance of a User Agency contract or program, the following rules shall apply:

a. If information is included in the proposal or other material which we identify as already being classified, the proposal or other material shall be marked with the appropriate classification.

b. If the case does not fall within paragraph a above, and we believe that the material contains information which may or should be safeguarded, protect the information as though classified at the appropriate level, until an advisory classification opinion is obtained from a User Agency which has an interest in the subject matter. In any such case, the following protective marking will be used:

**CLASSIFICATION DETERMINATION PENDING -**

**PROTECT AS THOUGH CLASSIFIED**

**(TOP SECRET, SECRET, OR CONFIDENTIAL)**

*This marking should appear conspicuously at least once on the material but no further markings are necessary until a classification determination is received.*

5. The fact that classified information has been made public does not mean that it is automatically declassified. Contractors shall continue the classification until formally advised to the contrary.

B. The DD Form 254

The security classification to be applied to information involved in a User Agency classified contract will be supplied to us by the Contracting Officer or the designated representative of the User Agency concerned. The DD Form 254 is the basic document used to convey the classification, regrading, downgrading, and declassification specifications for a classified contract.

Should our company issue a classified subcontract to another cleared facility, we are responsible for issuing accurate and current classification guidance in conjunction with a DD Form 254 as applicable to the classified work the subcontractor is tasked to do for us.

If you encounter difficulty in applying or interpreting classification guidance provided to us, contact the Security Officer and your Program Manager. A request for clarification or assistance will be submitted to the User Agency involved.

# SECTION 12

## MARKING CLASSIFIED MATERIAL

Classification designation by physical marking, notation or other means serves to warn and to inform the holder what degree of protection against unauthorized disclosure is required for that information or material. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. Therefore, it is essential that all classified information and material be marked in such a manner that it is clear to the holder what level of classification is assigned to the information or material, exactly what portions of the information or material contain or reveal classified information, how long the protection is required, and any other additional markings required for protection of the information or material.

Incoming classified material will be reviewed by the FSO for proper markings immediately upon its receipt. If any marking errors or omissions are noted, send a written request to the sender for a properly marked copy. Until a properly marked copy is received, add the following caveat to the cover sheet for the document:

**THIS DOCUMENT WAS RECEIVED FROM AN OUTSIDE SOURCE AND**

**DOES NOT HAVE ALL OF THE MARKINGS REQUIRED BY CHAPTER 4**

**OF THE NISPOM. PRIOR TO EXTRACTING ANY PORTION OF THIS**

**DOCUMENT FOR ANY PURPOSE CONTACT FSO OR DESIGNEE FOR GUIDANCE**

*Internally generated classified material will be properly marked immediately upon its creation.*

See the FSO should any questions arise concerning markings which are not answered by review of this section.

A. Marking Requirements for Information and Material

The markings shown in paragraphs 1 through 8 below are required for all classified information, regardless of the form in which it appears. Some material, such as documents, letters, and reports, can be marked easily with the appropriate markings. Marking other material, such as equipment, AIS media and slides, will be more difficult due to size or other physical characteristics. Since the purpose of the markings is to warn the holder that the information requires special protection, it is necessary that all classified material be marked with the appropriate markings to the fullest extent possible to ensure that it is afforded the necessary safeguards.

1. Identification Markings - all classified material shall be marked to show:

a. The name and address of the facility responsible for its preparation, and the date of preparation.

These markings are required on the face of all classified documents:

2. Overall Markings - the overall classification of a document, or any copy or reproduction thereof, shall be conspicuously marked or stamped at the top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). If the document does not have a back cover, the outside of the back or last page, which may serve as a cover, shall also be marked at the top and bottom with the overall classification of the document. The markings shall be stamped, printed, etched, written, engraved, painted, or affixed by means of a tag, sticker, decal, or similar device on classified material, other than documents, and on containers of such material, if possible. If marking the material or container is not practical, written notification of the appropriate markings shall be furnished to recipients. Copies of documents shall include the appropriate markings on the documents themselves.

3. Page Markings - interior pages of classified documents shall be conspicuously marked or stamped at the top and bottom with the highest classification of the information appearing thereon, or the designation UNCLASSIFIED, if all the portions on the page are UNCLASSIFIED. Alternatively, the overall classification of the document may be conspicuously marked or stamped at the top and bottom of each interior page, when necessary to achieve production efficiency and so that the particular information to which classification is assigned is adequately identified. In any case, the classification marking of a page shall not supersede a lower level of classification indicated by a portion marking applicable to information on that page.

4. Component Markings - the major components of complex documents are likely to be used separately. In such instances, each major component shall be marked as a separate document utilizing the classification marking requirements of the NISPOM. Examples include:

* Each annex, appendix, or similar component of a plan, program, or project description;
* Attachments and appendices to a letter;
* Each major part of a report.
* If an entire major component is UNCLASSIFIED, the first page of the component may be marked at the top and bottom with the designation “UNCLASSIFIED” and a statement included, such as, “All portions of this (annex, appendix, etc.) are UNCLASSIFIED.” When this method of marking is used, no further markings are required on the unclassified major component.

5. Portion Markings - each section, part, paragraph, or similar portion of a classified document shall be marked to show the highest level of its classification, or that such portion is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contains or reveals classified information. For the purpose of applying these markings, a portion of paragraph shall be considered a distinct section or subdivision of a chapter, letter, or document dealing with a particular point or idea which begins on a new line and is often indented. Classification levels of portions of a document shall be shown by the appropriate classification symbol placed immediately following the portion’s letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. In marking portions, the parenthetical symbols

* “(TS)” for TOP SECRET
* “(S)” for SECRET
* “©” for CONFIDENTIAL
* “(U)” for UNCLASSIFIED

shall be used. When appropriate, the symbols

* “RD” for RESTRICTED DATA
* “FRD” for FORMERLY RESTRICTED DATA

shall be added, for example, “(S-RD)” or “(C-RD)”. In addition, portions that contain Critical Nuclear Weapon Design Information (CNWDI) will be marked “(N)” following the classification, for example, “(TS-RD) (N)”.

a. Portions of U.S. documents containing foreign government information shall be marked to reflect the country or international organizations of the governments of origin as well as the appropriate classification,

(for example, “(NATO-S)” or “(UK-C)”, or “(NATO-R)” for NATO-RESTRICTED)

except where such markings would reveal that the information is foreign government information, when that fact must be concealed, or if a confidential source or relationship not otherwise evident in the document is revealed. Where a User Agency determines that this information would be revealed, the marking FGI-S, or FGI-C, etc. should be used.

b. When illustrations, photographs, figures, graphs, drawings, charts, or similar portions are contained in classified documents they shall be marked clearly to show their classified or unclassified status. In this instance, such markings shall not be abbreviated and shall be prominent and placed within or contiguous (touching or near) to such a portion. Captions of such portions shall be marked on the basis of their content alone by placing the symbol “(TS)’, “(S)”, “(C)”, or “(U)” immediately preceding the caption.

c. If, in an exceptional situation, parenthetical marking in the portion is determined to be impractical, the classified document shall contain a description sufficient to identify the exact information that is classified and the classification level(s) assigned to it. For example, each portion of a document need not be separately marked if all portions are classified at the same level, provided a full explanation is included in the document.

d. When elements of information in one portion or paragraph require different classifications, but segregation into separate portions or paragraphs would destroy continuity or context, the highest classification required for any item shall be applied to that portion or paragraph.

6. Subject and Title Markings - subjects and titles of documents shall be selected, if possible, so as not to require classification. A classified subject or title shall be marked with the appropriate symbol (TS), (S), or © placed immediately following and to the right of the item. An unclassified subject or title shall be marked with a (U) placed immediately following and to the right of the item. When applicable, other appropriate symbols, for example, “(RD)”, “(FRD)”, “(N)”, or “(NATO)” shall be added.

7. Downgrading/Declassification and “Classified by” Markings - procedures for marking downgrading and declassification instructions and for completion of the “Classified by” line are prescribed in Paragraph 4-208 of the NISPOM. These markings shall be placed either on the cover, first page, title page, or in a similarly prominent position on classified documents.

8. Additional Markings - in addition to the markings specified above, classified material shall be marked, if applicable, with one or more of the notations prescribed below, or other markings specified by a User Agency. The appropriate notation shall be printed, stamped, typed, or otherwise affixed conspicuously at least once on classified material possessed, prepared, or reproduced by the contractor. In addition, when a copy, extract, or paraphrase of a document contains classified information, or when a page, chapter, or other component is separated from such a document, the extract or component shall also be conspicuously marked at least once with the appropriate notation. In the case of documents, these warning notices shall be conspicuously marked on the outside of the front cover (if any), or on the first page if there is no front cover. When display of warnings notices on the materials is not feasible, the warnings shall be included in the written notification provided to recipients.

a. RESTRICTED DATA Notation - The following notation shall be affixed on all material which contains “RESTRICTED DATA”:

*RESTRICTED DATA*

*This material contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.*

b. FORMERLY RESTRICTED DATA - Notation Except when the “RESTRICTED DATA” notation is used, all material containing information in the “FORMERLY RESTRICTED DATA” category shall be marked with the following notation:

*FORMERLY RESTRICTED DATA*

*Unauthorized disclosure subject to administrative and criminal sanctions. Handle as RESTRICTED DATA in foreign dissemination. Section 144 b, Atomic Energy Act 1954.*

c. INTELLIGENCE INFORMATION - Intelligence information shall be marked in accordance with DCI Directive 1/7 last revised April 12, 1995.

*“DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR” (ORCON)*

This marking may be used only on classified intelligence that clearly identifies or would reasonably permit ready identification of intelligence sources or methods that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness.

*“CAUTION-PROPRIETARY INFORMATION INVOLVED” (PROPIN)*

This marking is used with or without a security classification, to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value.

*“NOT RELEASABLE TO FOREIGN NATIONALS” (NOFORN)*

Based on the unique dissemination requirements of some Intelligence Community organizations, this control marking may be used on intelligence that, if released to foreign governments or nationals, could jeopardize intelligence sources or methods, or when it would not be in the best interest of the United States. This control marking is used to identify classified intelligence that may not be released in any form to foreign governments, foreign nationals, or non-US citizens without permission of the originator. This marking may be abbreviated “NOFORN” or “NF”. It is not authorized for use in conjunction with the “AUTHORIZED FOR RELEASE TO” control marking described below.

“AUTHORIZED FOR RELEASE TO … (name of country(ies)/international organization)” REL or REL TO

This marking is used to identify classified intelligence that an originator has predetermined to be releasable or has been released, through established foreign disclosure procedures and channels, to the foreign country(ies)/international organization(s) indicated. This marking may be abbreviated “REL (abbreviated name of country (ies)/international organization)”.

The control markings authorized above shall be shown on the title page, front cover, and other applicable pages of documents, incorporated in the text of electrical communications, shown on graphics, and associated with data stored or processed in automated information systems. The control markings shall also be used in abbreviated form at the beginning or end of portions. If the control markings apply to all portions, the document may be marked with a statement to this effect rather than marking each portion individually.

*OBSOLETE CONTROL MARKINGS FOR INTELLIGENCE INFORMATION*

The control markings, Warning Notice-Intelligence Sources or Methods Involved (WNINTEL) and Not Releasable to Contractors/Consultants (NOCONTRACT) are no longer authorized for use after April 12, 1995. Remarking of material bearing the “WNINTEL” and “NOCONTRACT” control marking is not required. Holders of material bearing these markings may line through or otherwise remove the marking from documents or other material.

d. FOREIGN GOVERNMENT INFORMATION - this marking is used on U.S. documents containing “FOREIGN GOVERNMENT INFORMATION” to ensure that such information is not declassified prematurely or made accessible to nationals of a third country without the consent of the originator.

e. NATO INFORMATION

- THIS DOCUMENT CONTAINS NATO INFORMATION: This marking is used on U.S. documents that contain extracts from NATO documents to ensure that such information is not declassified or made accessible to nationals of non-NATO countries without NATO approval.

- All NATO classified documents created by this facility must be portion marked. Any portion extracted from a NATO document that is not portion marked, must be assigned the classification that is assigned to the NATO document.

All U.S. originated NATO classified documents shall bear an assigned reference number and date on the first page. The reference numbers shall be assigned as follows:

1. The first element shall be the abbreviation for the name of the contractor facility.
2. The second element shall be the abbreviation for the overall classification followed by a hyphen and the four digit sequence number for the document within that classification that has been generated for the applicable calendar year.
3. The third element is the year; e.g., MM/NS-0013/95.

- COSMIC TOP SECRET, NATO SECRET and ATOMAL documents must bear the reference number on each page and a copy number on the cover or first page. Copies of NATO documents must be serially numbered. Pages shall be numbered. The first page or index or table of contents shall include a list, including page numbers, of all Annexes and Appendices. The total number of pages shall be stated on the first page. All Annexes or Appendices will include the date of the original document and the purpose of the new text (addition or substitution) on the first page.

- One of the following markings must be applied to NATO documents that contain ATOMAL information:

1. “This document contains U.S. ATOMIC Information (RESTRICTED DATA or FORMERLY RESTRICTED DATA)) made available pursuant to the NATO Agreement for Cooperation Regarding ATOMIC Information, dated 18 June 1964, and will be safeguarded accordingly.”

2. “This document contains UK ATOMIC Information. This information is released to the North Atlantic Treaty Organization including its military and civilian agencies and member states on condition that it will not be released by the recipient organization to any other organization or government or national of another country or member of any other organization without prior permission from H.M. Government in the United Kingdom.”

B. Marking Specific Types of Material

The following procedures for marking specific types of material are not all inclusive. Due to the many variations that may occur in the preparation of classified materials, every possible marking situation cannot be addressed. These procedures are for marking various types of material, which are most often encountered by contractors, and may be varied to accommodate the physical characteristics of the material and organizational and operational requirements.

1. Artwork

Original artwork shall have the overall security classification stamped or conspicuously marked in the top and bottom margins of the mounting board and on all overlays and cover sheets. Other markings specified in Paragraphs A-1 through A-7 above, also shall be included on such documents, as applicable.

2. Charts, Maps, Drawings, and Tracings.

The appropriate classification markings for the legend, title, or scale block shall be shown in the legend, title or scale block itself, or in such a manner as to differentiate between the overall classification assigned to the document and any classification assigned to the legend or title itself. The overall classification of the document shall be marked or stamped at the top and bottom of each document. Any identifiable portions of such documents shall be marked in the manner prescribed in Paragraph A-5 above, if possible. When the customary method of folding or rolling charts, maps, drawings, or tracings would cover the classification markings, additional classification markings shall be placed so as to be clearly visible when the document is folded or rolled. Other markings specified in paragraphs A-1 through A-7 above also shall be included on such documents, as applicable.

3. Decks of Automatic Data Processing Punched Cards

When a deck of classified AIS punched cards is handled and controlled as a single document, only the first and last cards of the deck require the overall classification markings. An additional card shall be added (or job control card modified) to identify the contents of the deck, and to show the appropriate markings specified in paragraphs A-1 through A-7 above. Individual cards removed for separate processing or use, and not immediately returned to the deck, shall be protected to show the appropriate markings specified in Paragraph A-1 through A-7 above. Alternatively, a grouping of cards removed for separate processing or use, and not immediately returned to the deck, may be handled, controlled, and marked as a separated deck of cards.

4. Files, Folders, or Groups of Documents

Files, folders, binders, envelopes, and other items, containing classified documents, when not in secure storage, shall be conspicuously marked according to the highest classification of any classified document included herein. Classified document cover sheets may be used for this purpose.

5. Messages

Electronically transmitted messages (that is, those transmitted via authorized CRYPTOSYSTEMS) shall bear appropriate markings as specified in paragraphs A-1 through A-7 above, except as noted herein. The first item of information in the text shall be the overall classification of the message. The message shall show the date or event for declassification or the notation “Originating Agency’s Determination Required” or “OADR”, and downgrading action, if applicable. The “Classified by” line information is not required. Portions shall be marked in the manner required for other documents. When messages are printed by an automated system, all markings may be applied by that system, provided that the classification markings are clearly distinguished from the printed text.

NOTE: The highest level official identified on the message as the sender, or in the absence of such identification, the highest level official at the facility originating the message, is deemed to be the classifier of the message. The originator is responsible for maintaining adequate records to show the source of an assigned derivative classification.

6. Microforms

Microforms are copies usually produced on transparent or opaque materials in sizes too small to be read by the unaided eye. Accordingly, the appropriate markings as specified in Paragraph A-1 through A-7 above shall be conspicuously marked on the microform medium or its container, so as to be readable by the unaided eye. These markings shall also be included on the image so that when the image is enlarged and displayed or printed, the markings will be conspicuous and readable. The markings may be abbreviated. Further markings and handling shall be as appropriate for the particular microform involved. For example, roll file microforms may generally be handled as provided for roll motion picture films, and decks of “aperture cards” may be handled as decks of automatic data processing punched cards. Whenever possible, microfiche, microfilm strips, and microform chips shall be handled in accordance with this paragraph.

7. Motion Picture Films

Classified motion picture video tapes shall be marked at the beginning and end of each reel by titles bearing the appropriate classification and applicable associated markings. Such markings shall be visible when projected. Motion picture film and video tape containers shall bear conspicuous classification, declassification, and if applicable, downgrading markings. Other markings specified in this procedure shall be applied, if applicable.

8. Photographs

Photographs shall be marked in such a manner so that a recipient or viewer will know that information of a specified level of classification is involved. Negatives and positives shall be marked, whenever practical, with the appropriate classification and applicable associated markings. Roll negatives or positives may be so marked at the beginning and end of each strip. Containers for negatives and positives shall be conspicuously marked with the highest level of classification of their contents. Other markings specified in this procedure shall be applied, if applicable. All prints and reproductions shall be conspicuously marked with the appropriate markings on the face side of the print, if possible. Where such markings cannot be applied to the face side, or affixed by pressure tape label, stapled strip, or other comparable means.

NOTE: When self-processing film or paper is used to photograph or reproduce classified information, all parts of the last exposure shall be removed from the camera and destroyed as classified waste.

9. Recordings

Magnetic, electronic, or sound recordings shall contain a clear statement of the overall classification at the beginning and end of the recording which will provide adequate assurance that any listener or receiver will know that classified information is involved. Containers for recordings shall be conspicuously marked with the appropriate classification and applicable associated markings.

10. Removable Automatic Data Processing and Word Processing Storage Media

a. External Removable information storage media and devices, employed with AIS’s shall bear external markings clearly indicating the appropriate markings. Included are media and devices that store recorded information in analog or digital form, and are generally mounted or removed by the users or operators. Examples include magnetic tape reels, cartridges and cassettes; removable disks, disk cartridges, disk packs, and diskettes; paper tape reels; magnetic cards.

b. Internal In addition, AIS’s employing such media shall provide for internally recorded security markings to ensure that classified information contained therein, when reproduced or generated will bear appropriate markings.

11. Translations

Translations of U.S. classified information into a language other than English shall be marked to show the U.S. as the country of origin, with the appropriate U.S. markings as specified in this procedure.

12. Transmittal Documents

A transmittal document, including endorsements and comments when such are added to the basic communication, shall carry on its face a prominent notation as to the highest classification of information transmitted by it and a legend showing the classification, if any, of the transmittal document, endorsement, or comment standing alone. For example, an unclassified document that transmits as an attachment to a classified document shall bear a notation substantially as follows: “Unclassified when separated from classified enclosures.”

13. Transparencies and Slides

Applicable classification markings shall be shown clearly on the image of each transparency or slide, and on its border, holder, or frame. Other applicable markings as specified shall be shown on the border, holder, or frame, if possible, or in the image area, in accompanying documentation, or other written notification. When a set of transparencies or slides is handled and controlled as a single document, only the title slide or transparency requires the other applicable markings. Slide and transparency storage containers shall also be marked with the applicable markings as specified in this procedure.

14. Miscellaneous Materials

Unless a requirement exists to retain material such as rejects, typewriter ribbons, carbons and similar items for a specific purpose, there isn’t a need to mark, stamp, or otherwise indicate that the information is classified.

NOTE: Such material developed in connection with the handling, processing, production, and utilization of classified information shall be handled in a manner that ensures adequate protection of the classified information involved and destruction at the earliest practical moment.

C. Marking of Regraded Documents and Material

Whenever classified information is downgraded, declassified, or upgraded, the material shall be promptly and conspicuously marked to indicate the change.

1. Automatic Downgrading or Declassification Actions

Holders of classified material may take automatic downgrading or declassification actions, as specified by the markings on the material, without further authority for the action. All old classification markings shall be canceled and the new markings substituted, whenever practical.

a. In the case of documents, as a minimum, the outside of the front cover (if any), the title page (if any), the first page and the outside of the back cover (if any), must reflect the new classification markings, or the designations UNCLASSIFIED.

b. Other material shall be re-marked by the most practical method for the type of material involved to ensure that it is clear to the holder what level of classification is assigned to the material. Old markings shall be canceled, if possible, on the material itself. If not practical, the material may be marked by affixing new decals, tags, stickers, and the like to the material or its container.

2. Other than Automatic Downgrading or Declassification Actions

When contractors are notified of downgrading or declassification actions that are contrary to the markings shown on the material, the material shall be remarked to indicate the change. All old classification markings shall be canceled and the new markings substituted, whenever practical.

In the case of documents, as a minimum, the outside of the front cover (if any), the title page (if any), the first page, and the outside of the back cover (if any) shall reflect the new classification markings or the designation UNCLASSIFIED. In addition, the material shall be marked to indicate the authority for the action, the date of the action, and the identity of the person or contractor taking the action. Other holders shall be notified if further dissemination has been made by the contractor.

3. Upgrading Action

When a notice is received to upgrade material to a higher level, for example from CONFIDENTIAL to SECRET, or from UNCLASSIFIED to CONFIDENTIAL, the new markings shall be immediately entered on the material, in accordance with the notice to upgrade, and all the superseded markings should be canceled, if applicable. Other holders shall be notified, if further dissemination of the material has been made by the contractor. If contractor-generated material is inadvertently distributed outside the facility without the proper classification assigned to it, or without any markings to identify the material as classified, the following procedures apply:

a. Determine that all holders of the material are authorized access to it. If the recipients are cleared for access to the material, promptly provide written notice to all holders of the proper classification to be assigned. If all copies cannot be accounted for, or if unauthorized personnel have had access to it, report the compromise to the FSO.

b. In the case of classified material being upgraded, the written notice to the recipients shall not be classified unless the notice contains additional information warranting classification. In the case of material which was inadvertently released as unclassified, the written notice shall be classified CONFIDENTIAL, unless it contains additional information warranting a higher classification.

D. Marking of Foreign Classified Material

Foreign classified material shall be marked in accordance with instructions received from the foreign contracting authority, the CSO, or the UA. In any case, if the classification and the country of origin are in a language other than English, the appropriate equivalent U.S. classification and the country of origin will be marked on the foreign classified material. Except for the foreign security classification designation RESTRICTED, foreign security classification designations, including those of international organizations of governments, such as NATO, generally parallel U.S. classification designations. A table of foreign equivalent classifications is contained in Appendix F.

E. Marking Wholly Unclassified Material

Normally, wholly UNCLASSIFIED material will not be marked or stamped “UNCLASSIFIED” unless it is essential to convey to a recipient of such material that:

1. The material has been examined specifically with a view to impose a security classification and has been determined not to require classification, or

2. The material has been reviewed and has been determined to no longer require classification and it is declassified.

F. Marking Compilation

1. Documents - in some instances, certain information that would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification assigned to the document shall be conspicuously marked or stamped at the top and bottom of each page and on the outside of the front and back covers, if any. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the document. In this instance, the portions of a document classified in this manner need not be marked.

2. Portions of a Document - if a classified document contains certain portions that are unclassified when standing alone, but classified information will be revealed when they are combined or associated, those portions shall be marked as UNCLASSIFIED, the page shall be marked with the highest classification of any information on the page, and a statement shall be added to the page, or to the document, to explain the classification of the combination or association to the holder. This method of marking may also be used if classified portions on a page, or within a document, will reveal a higher classification when they are combined or associated than when they are standing alone.

# SECTION 13

## DISPOSITION OF CLASSIFIED MATERIAL

A. Ongoing Program of Reduction

Remember that Management’s goal regarding disposition is to reduce to the absolute minimum the quantity of classified material on hand at any given time. Security will supply, to the necessary management personnel a listing of documents on a continuing basis for review of holdings which are no longer needed. Security will ensure that classified holdings are destroyed or returned as soon as practical, after the material has served the purpose for which it was:

1. Released by the Government

2. Developed or prepared by a contractor, or

3. Retained after completion of the contract

The Facility Security Officer will closely evaluate the promptness and effectiveness of the facility’s disposition actions during each self-inspection.

Disposition requirements apply equally to all reproductions of classified information as well.

During self-inspections, our FSO will place particular emphasis on the elimination of excess copies, declassification of unnecessary holdings on AIS media, disposition of classified waste, and destruction of information which was incorporated into later documents/reports.

B. Means of Disposition

At no time shall our employee’s dispose of classified material. All classified material needing disposition, shall be brought to Security. Security will dispose of all classified material by:

1. Returning the classified material to the customer (if specifically requested or directed),

2. Destruction by authorized means, unless specifically prohibited,

3. Transfer to a follow-on or related active contract by written authority.

4. Retention unrelated to an active procurement for a specific period of time by written authority.

5. All written authorizations must be kept on file.

C. Responsibilities for Disposition of Classified Material Related to Solicitations and Contracts

1. Contracts Administration or the Program Manager will notify Security immediately when:

a. The decision is made not to submit a bid for a classified job or to withdraw such a bid.

b. Notified that a bid, proposal, or quote for classified work has not been accepted.

c. The final goods and services have been delivered to the customer on a classified contract. This includes the final report.

d. A classified contract is terminated by the Government or prime contractor prior to completion of the effort.

2. The FSO will immediately return or destroy all the residual classified material when any of the following occurs:

* 1. If a bid, proposal, or quote is not submitted or is withdrawn—within 180 days after the opening date of bids, proposals, or quotes.

b. If a bid, proposal, or quote is not accepted—within 180 days after notification.

c. If we were a successful bidder and a prime contractor - two years after final delivery of goods and services. If we were a subcontractor, and received retention for two years after final delivery of goods and services.

3. If you wish to retain classified material received or generated under the contract you may do so for a period of two years after completion of the contract, provided the User Agency Contracting Officer does not advise to the contrary. If you wish to retain any of the material for a period beyond the two year retention period prepare a memo justifying the retention request and return it to the FSO. Identify the accountable classified material by attaching a listing of the specific documents involved. Specify an active procurement for a transfer request and a period of time (not to exceed five years) for a retention request. Fully explain in detail, how the transfer or retention will assist our company and benefit the Government in performance on other contracts. If the Program Manager does not fully justify the request, the FSO will not prepare the request for retention, or transfer.

4. If we are a prime or subcontractor the two year retention of classified material under the completed contract is automatic, unless advised otherwise.

5. If you wish to retain the classified material beyond the two year period, the FSO will forward a letter of request to the User Agency Procuring Contracting Officer (PCO) where we are the Prime contractor. Where we are a subcontractor, send the request through the prime contractor.

1. Requests for transfer of contract-related and other classified reference material are addressed to the Contracting Officer of the active procurement. Upon approval, the material becomes associated with and is administered under the current procurement.
2. Requests for retention of contract-related material are addressed to the Contracting officer of the completed procurement.

D. Responsibilities for Disposition of Other Classified Material

1. Our facility will also receive classified “field of interest” material which is not related to a proposal or contract. Such material includes classified bibliographies, seminar/symposium notes and reports, long range scientific and technical planning programs, planning briefings for industry, unsolicited proposals, independent research projects and marketing information reports.

2. Whenever one of our employees is offered such classified material (at a military installation, contractor’s site, symposium, etc.), our employees will insist that the material be mailed to our classified mailing address and to the attention of our FSO. Immediately notify the FSO of its impending shipment.

3. When the material arrives, the FSO will complete all the actions required for incoming classified transmissions. In addition, the FSO will establish a suspense file to review the field of interest material one year from date of receipt.

4. One year from the date of receipt at our facility, the FSO will contact the employee for whom the material was received. If there is a continuing need to use the material, the employee will prepare a fully justified transfer/retention request using similar criteria to those described above of contractually-related classified material. Submit this request to the FSO.

5. Address such requests to an official of the User Agency which authorized release of the information. Follow the guidance above for contract related material.

6. If our employee does not prepare an adequate justification for retention within 1 year after the material was received, the FSO will destroy or return the material.

E. Destruction of Classified Material

1. Control - Our FSO will designate in writing individuals who are appointed to destroy classified material.
   1. For destruction of Secret and Confidential material one person cleared to the highest level of the material to be destroyed is needed.
   2. Destruction officials and witnesses, if required, must be cleared to the level of the material to be destroyed. Personnel holding clearances with limitations may not destroy material to which they are precluded from access.
2. Destruction of Classified Waste
   1. Destroy classified waste as soon as practical but, in no case, not more than one month after it has served its purpose.
   2. All waste material must be safeguarded according to its classification at all times. This includes all waste material containing classified information—preliminary drafts, carbon sheets, typewriter and printer ribbons, plates, stencils, masters, stenographic notes, worksheets, etc.
   3. Classified waste awaiting destruction will be conspicuously marked with the most restrictive classification of the material and will be segregated from other material in the storage container. Folders, envelopes, and “burn bags” used for this purpose must be conspicuously marked on the outside surface.

3. Methods of Destruction

Any method of destruction for classified material we use must be approved by the Security Office first. Classified material may not be destroyed at another location other than this facility without the prior approval of DSS.

Paper Products

Classified material through Secret may be destroyed by one of these methods only:

1. Crosscut shredders may be used when the residue is no larger the 1/32” in width (with a plus tolerance of 1/64”) by ½” length. If the trial residue exceeds these tolerances, adjust the machine until satisfactory results are obtained. Microfilm, microfiche, and other high density materials must not be processed in the shredder.
2. Paper may also be destroyed by pulping, pulverizing and burning.

AIS Magnetic Media

AIS magnetic media - mag tapes and floppy disks, classified through the level of Secret, will be destroyed according to the procedures approved in the Security Plan for the AIS.

Other Materials

1. Other materials may be destroyed by melting, mutilation, chemical decomposition or burning.

# SECTION 14

## REPRODUCTION OF CLASSIFIED MATERIAL

Reproductions of Confidential and Secret material may be made only if they are essential to the:

* Performance of a prime or subcontract.
* Preparation of a solicited or unsolicited bid, quotation, or proposal to a U.S. Government User Agency or prospective subcontractor.
* Preparation of patent applications to be filed in the U.S. Patent Office.
* **And** reproduction is not restricted by a Government Contracting Authority.

If any reproduction is approved, only personnel authorized do so will make copies. Records of the reproduction of Secret and Confidential material are not required unless requested by the Government Contracting Authority. If it is necessary to have reproduction done by a graphic arts company, the Security Officer will ensure that all requirements are met concerning access controls and subcontracting.

All reproductions of classified material shall be conspicuously marked with the same classification markings as the material being reproduced. Copies of the classified material must be reviewed after the reproduction process to ensure that these markings are visible.

Only copiers authorized by the security officer may be used for classified reproduction. The classified material being reproduced must remain under the control of a cleared and authorized employee at all times during the copy process. After the reproduction is complete, the copier should be thoroughly checked to ensure all classified material has been removed from it.

# SECTION 15

## REQUIREMENTS FOR TOP SECRET MATERIAL

A. Control and Accountability

TOP SECRET control officials must be designated to receive, transmit, and maintain access and accountability records for TOP SECRET information. An inventory must be conducted annually unless written relief is granted by the Government Contracting Authority.

The transmittal of TOP SECRET information must be covered by a continuous receipt system both within and outside our facility.

Each item of TOP SECRET material must be numbered in series. The copy number will be placed on all TOP SECRET documents and on all associated transaction documents.

B. Generation of TOP SECRET Material

If our facility generates TOP SECRET material a record must be made when the material is (1)Completed as a finished document; (2) Retained for more than 30 days after creation, regardless of the stage of development; or (3) Transmitted outside the facility.

C. Storage of TOP SECRET Material

All TOP SECRET material must be stored in a GSA-approved security container, an approved vault or an approved closed area. Supplemental protection is required.

D. Transmission of TOP SECRET Material

Only the FSO, with the written authorization of the Government Contracting Authority is authorized to transmit TOP SECRET material outside of this facility. TOP SECRET material may be transmitted by the following methods within and directly between the U.S., Puerto Rico, or a U.S. possession or trust territory.

1. The Defense Courier Service (DCS), if authorized by the GCA.

2. A designated courier or escort cleared for access to TOP SECRET information.

3. By electrical means over government approved secured communications security circuits provided such transmission conforms with the NISPOM, the telecommunications security provisions of the contract, or as otherwise authorized by the GCA.

For transmission outside the U.S., Puerto Rico, or a U.S. possession or trust territory, TOP SECRET may be transmitted by the Defense Courier Service, Department of State Courier System, or a courier service authorized by the GCA.

E. Reproduction of TOP SECRET material

TOP SECRET documents may be reproduced as necessary in the preparation and delivery of a contract deliverable. Reproduction for any other purpose requires the consent of the GCA.

A record must be maintained of the reproduction of all TOP SECRET material for no less than two years.

F. Disposition of TOP SECRET material

For the destruction of TOP SECRET material, two persons must be present. A record of the destruction is required and it must include (1) The date of the destruction; (2) Identity of the material destroyed; (3) Signatures of the individuals designated to destroy and witness the destruction. Destruction officials must know through their personal knowledge, that such material was destroyed. Destruction records must be maintained for no less than two years.

# SECTION 16

## SPECIAL REQUIREMENTS FOR RESTRICTED DATA

SPECIAL REQUIREMENTS FOR RESTRICTED DATA, FORMERLY RESTRICTED DATA, DoD CRITICAL NUCLEAR WEAPON DESIGN INFORMATION, NATO, COMSEC AND INTELLIGENCE INFORMATION

A. Restricted Data and Formerly Restricted Data

Restricted Data and Formerly Restricted Data is atomic energy information that is classified under the authority of the Atomic Energy Act of 1954 and is under the jurisdiction and control of the Department of Energy (DOE). Either the DOE or Nuclear Regulatory Commission (NRC) may inspect and monitor any programs of ours that include access to this type of information or through written agreement with the DoD; DSS may inspect and monitor these programs.

RESTRICTED DATA (RD) means all data concerning, (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142.

FORMERLY RESTRICTED DATA (FRD) is information which has been removed from the Restricted Data category after the DOE and the DoD have jointly determined that the information relates primarily to the military utilization of atomic weapons and can be adequately safeguarded as National Security Information in the United States. Such data may not be given to any other nation except under specially approved agreements and with the authorization of DOE. FRD is identified and handled as Restricted Data when sent outside of the United States.

Our facility must report all unauthorized disclosures involving RD and FRD to DSS. Disclosure of FRD and RD to Foreign Nationals is not authorized.

The minimum investigative requirements and standards for access to RD and FRD are:

* Top Secret RD: A favorable Single Scope Background Investigation (SSBI)
* Secret RD: A favorable SSBI
* Confidential RD: A favorable NACC
* Top Secret FRD: A favorable SSBI
* Secret FRD: A favorable NACC
* Confidential FRD: A favorable NACC

All Restricted Data information is born classified; therefore, no classification category determination by a person with original classification authority is ever required for RD or FRD. No date or event for automatic declassification ever applies to RD or FRD. If our facility should develop RD, FRD, or an invention or discovery useful in the production or utilization of special nuclear material or atomic energy, we must file a report with a complete description thereof with the DOE or the commissioner of Patents as prescribed by the Act. Documents thought to contain RD or FRD shall be marked temporarily as such.

* For additional requirements see the NISPOM Sap Supplement.

B. DOD Critical Nuclear Weapon Design Information

Critical Nuclear Weapon Design Information or CNWDI is a DOD category of TOP SECRET Restricted Data or Secret Restricted Data that reveals the theory of operation of design of the components of a thermonuclear or fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fissionable, and high explosive materials by type.

The sensitivity of DOD CNWDI is such that access shall be granted to the absolute minimum number of employees who require it for the accomplishment of assigned responsibilities on a classified contract.

Briefings: Prior to accessing DOD CNWDI, employees must be briefed on its sensitivity by the FSO or alternate. Upon termination of access to CNWDI, employees will be given an oral debriefing.

Subcontractors: Our facility is not allowed to disclose CNWDI to subcontractors without the prior written approval of the GCA.

Transmission: Transmission of such material outside of this facility is only authorized to the GCA or a subcontractor if approved by the GCA. Prior to any transmittal, verification must be obtained from DSS that the receiving facility is authorized access to CNWDI. Only the FSO will be authorized to transmit CNWDI material.

Records: A record must be maintained of all employees who have been authorized access to CNWDI and the date of CNWDI briefings. Such records will be maintained for no less than two years from the date of termination of the person’s access to CNWDI.

C. NATO Information

NATO information belongs to the North Atlantic Treaty Organization and has four levels of security classification:

* COSMIC TOP SECRET (CTS)
* NATO SECRET (NS)
* NATO CONFIDENTIAL (NC)
* NATO RESTRICTED (NR)

Another marking, ATOMAL, is applied to U.S. Restricted Data or Formerly Restricted Data and United Kingdom Atomic information that has been released to NATO. ATOMAL information is marked COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA).

NATO Facility Security Clearance Certificate- A NATO Facility Security Clearance Certificate is required for a contractor to negotiate or perform on a NATO classified contract. A U.S. facility qualifies for a NATO FSCC if it has an equivalent U.S. FCL and its personnel have been briefed on NATO procedures. A NATO FSCC is not required for Government Contracting Activity contracts that involve access to NATO classified information.

PCL Requirements- Access to NATO classified information requires a final PCL at the equivalent level. A PCL is not required for access to NATO RESTRICTED information.

NATO Briefings- Prior to having access to NATO classified information including Restricted; personnel must be given a NATO security briefing. When access to NATO classified information is no longer required, a debriefing must be given. A record of both briefings and debriefings will be made and retained for two years for NATO Secret, Confidential and Restricted, and three years for COSMIC TOP SECRET and all ATOMAL information. All personnel with NATO access, will receive annual refresher briefings as well.

Subcontracting for NATO contracts- Prior to awarding a NATO subcontract, we must obtain prior written approval from the NATO contracting activity and a NATO FSCC must be issued. A request for approval should be submitted through the cognizant DSS office.

Classification Guidance- Classification guidance will be provided in the form of a NATO security aspects letter and a security requirements checklist for NATO contracts, or a Contract Security Classification Specification. If adequate classification guidance is not received, the cognizant DSS office should be contacted.

Disclosure- We may not release or disclose NATO classified information to a third party or outside of our facility without the prior written approval of the contracting agency.

Storage- NATO documents shall be stored as prescribed for U.S. documents of an equivalent classification level with the following conditions:

* NATO classified documents cannot be commingled with other documents. NATO RESTRICTED documents may be stored in locked filing cabinets, bookcases, desks, or other locked containers that deter unauthorized access.
* In addition to the requirements for changing combinations to classified containers for U.S. classified material, NATO combinations must also be changed annually.
* All records of NATO combinations must be marked with the highest classification level of documents stored and must indicate the type and level of NATO documents in the container. The combination record must be logged and controlled in the same manner as NATO classified documents.

Reproduction - Our facility may reproduce NATO SECRET, CONFIDENTIAL and RESTRICTED documents to meet contractual requirements, as long as the contracting entity has not prohibited it.

Disposition- Generally, all NATO classified documents are returned to the contracting activity that provided them, upon completion of the contract.

Accountability Records- Logs, receipts, and destruction certificates are required for NATO classified information. Records for NATO documents must be maintained separately from records of non-NATO documents. COSMIC TOP SECRET and all ATOMAL documents must be recorded on logs maintained separately from other NATO logs and be assigned unique serial control numbers. Disclosure records bearing the name and signature of each person that has access are required for all COSMIC TOP SECRET, COSMIC TOP SECRET ATOMAL, and all other ATOMAL or NATO classified documents to which special access limitations have been applied.

As a minimum, our accountability record, receipts and destruction certificates must show the NATO reference number, short title, date of the document, classification, and serial copy numbers. The record must show the short title, unclassified subject, and distribution of the documents.

Receipts are required for all NATO classified documents, except NATO CONFIDENTIAL and RESTRICTED.

We will conduct an annual inventory of all COSMIC TOP SECRET, NATO SECRET and all ATOMAL documents.

Destruction certificates are required for all NATO classified documents except RESTRICTED. A witness is required for all COSMIC TOP SECRET, NATO SECRET and all ATOMAL documents.

Records will be retained for ten years for COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL documents and three years for NATO SECRET, NATO SECRET ATOMAL, NATO CONFIDENTIAL, and NATO CONFIDENTIAL ATOMAL documents.

Reporting security violations- Any loss, compromise, suspected loss or compromise, and security violations involving NATO classified information must be reported immediately to the FSO.

Extracting from NATO documents- The Central United States Registry must authorize any extraction from a COSMIC TOP SECRET or ATOMAL document.

If extracts of NATO information are included in a U.S. document prepared for a non-NATO contract, the document must be marked with U.S. classification markings. The caveat, “THIS DOCUMENT CONTAINS NATO (level of classification) INFORMATION” must be marked on the front cover or first page, of the document. Additionally, each paragraph or portion containing the NATO information must be marked with the appropriate NATO classification, abbreviated in parentheses. The “Declassify on” line of the document must show “Originating Agency Determination Required” or “OADR” unless the original NATO document shows a specific date for declassification. The declassification or downgrading of NATO information in a U.S. document requires the approval of the originating NATO activity.

NATO visits - a NATO Certificate of Security Clearance must be included with each request for NATO visit. Our visitor record must clearly identify NATO visitors, including those by U.S. personnel assigned to NATO. The records must be maintained for three years.

D. COMSEC Information

COMSEC or Communications Security refers to protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications. See the FSO for instructions on handling COMSEC materials. A COMSEC supplement to the NISPOM describes the security requirements for COMSEC information.

E. INTELLIGENCE Information

Intelligence information is information that is under the jurisdiction and control of the Director of Central Intelligence or a member of the Intelligence Community. The Intelligence Community as identified in Executive Order 12333 is: the Central Intelligence Agency (CIA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); offices within the DOD for the collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research (INR) of the Department of State; the intelligence elements of the Army, Navy, Air Force and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy (DOE); and the staff elements of the Director of Central Intelligence (DCI).

Intelligence Information includes the following classified information: (1) Foreign intelligence and counterintelligence as defined in E.O. 12333; (2) Information describing U.S. foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained for exploitation; and photography or recordings resulting from U.S. intelligence collection efforts; and (3) Information on Intelligence Community protective security programs (e.g., personnel, physical, technical, and information security).

Release of Intelligence Information- Intelligence information is released on a strict need-to-know basis. Prior written authorization must be obtained from the releasing Government Agency prior to disclosing intelligence information to another contractor.

Control of Intelligence Information - Special handling requirements and disposition instructions will be provided by the releasing agency.

Intelligence Information is not releasable to Foreign Nationals without prior written authorization of the originator.

# SECTION 17

## INTERNATIONAL SECURITY REQUIREMENTS

The transfer of articles and services, and related technical data, to a foreign person, within or outside the U.S., or the movement of such material or information to any destination outside the legal jurisdiction of the U.S., constitutes an export. Depending on the nature of the articles or data, most exports are governed by the Arms Export Control Act, the Export Administration Act and the Atomic Energy Act. A Foreign Person is defined as any foreign interest and any U.S. person effectively owned or controlled by a foreign interest.

Our Facility Security Officer and Export Control Officer must be contacted at the earliest feasible time when our facility intends to engage in any business, agreement, etc. with a foreign interest. Employees who are expected to be in personal contact with foreign interests must receive appropriate briefings from the FSO beforehand.

All requests for disclosure of U.S. classified or unclassified export controlled information to a foreign interest will be coordinated with the FSO and Export Control Officer.

A. Disclosure of U.S. Information to Foreign Interests

When information is derived from classified source material, is related to a classified Government Contracting Activity contract, and it has not been approved for public disclosure, advance disclosure authorization is required for release to a foreign entity. Disclosure may be through providing material or through oral discussions with a foreign interest. Disclosure authorization may be in the form of an export license, a letter of authorization from the U.S. Government licensing authority, or an exemption to the export authorization requirements. With the FSO’s support, our company’s export control officer and the appropriate program manager or designee will be responsible for obtaining the required authorization if it becomes necessary.

Sales, Loans, Leases, or Grants of Classified Items- Disclosure of classified information or release of classified articles or services in connection with Government sales, loans, eases, or grants shall be in accordance with security arrangements specified by the GCA.

Direct Commercial Sales- The disclosure of classified information may be authorized pursuant to a direct commercial sale only if the proposed disclosure is in support of a U.S. or foreign government procurement requirement, a Government contract, or an international agreement. A direct commercial sale includes sales under a government agency sales financing program.

Foreign Contractor Participation in U.S. Classified Contracts- Requests initiated by foreign contractors for classified information shall be submitted through the foreign country’s embassy in Washington, DC, to the GCA foreign disclosure office. Approval of the request by GCA does not alleviate the requirement for a U.S. contractor to obtain export authorization.

B. Foreign Government Information

Our facility must notify the Cognizant DSS Security Office when a classified contract is awarded by a foreign interest. Foreign government information must retain its original classification markings or will be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Some foreign governments have a fourth level of classification, RESTRICTED, for which there is no equivalent U.S. classification. The following guidance must be used when handling Foreign Government Information (FGI) Restricted:

1. Facilities must be appropriately cleared in accordance with the NISPOM prior to being given access to Restricted FGI.

2. Release to a third government national, government, etc. requires the prior written authorization of the originating government.

3. Personnel security clearances are not required unless the originating government specifically requires it. (A PCL is required for access to Spanish Restricted information). Prior to permitting an uncleared employee to access FGI Restricted, a briefing must be provided and the employee must acknowledge in writing his/her responsibilities for protecting the information.

4. The information may not be left unattended or handled in a manner that will allow unauthorized access to it. It may be stored in any lockable container that will preclude unauthorized persons access to it. When it is not secured in a container it will be turned face down or covered with a cover sheet that identifies it as Restricted Information.

5. Material containing Restricted information may be transmitted within the U.S. by any of the means authorized for CONFIDENTIAL information. First Class Mail may also be used with the following condition: the envelope or wrapper must be marked: “POSTMASTER: Address Correction Requested/Do Not Forward”. Double envelopes or wrappings are not required; however, the wrapping must be opaque. Receipts are not required unless required by the originating government.

6. The international transmission of Restricted will be through government to government channels, except as otherwise authorized in writing by a responsible security official of the originating government.

7. Transmitting Restricted by telephone or facsimile within the U.S. shall be by secure communications. If an urgent contract-related need develops, and secure communications are not reasonably available, non-secure communications may be used with the consent of the FSO. Such transmission internationally will be by secure communications unless authorized otherwise by the originating government.

8. FGI Restricted will be destroyed by any method approved for the destruction of classified information. A record of destruction is not required.

9. FGI Restricted will be processed and stored in AIS accredited for classified information.

10. FGI Restricted will be reproduced only as is necessary in support of a contract.

11. Violations of procedures for handling FGI Restricted must be reported to the FSO.

* Foreign government classification designations and the U.S. equivalents are shown in Appendix F.

U.S. documents that contain foreign government information shall be marked on the front, “THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT (indicate level) INFORMATION.” In addition, the portions must be marked to identify the classification level and the country of origin.

Foreign government classified material must be controlled and safeguarded in the same manner as U.S. classified material. It should not be commingled with other material. Access to it is restricted to only those employees with the appropriate level U.S. PCL and need-to-know. All foreign government classified material in our facility will be under our facility’s control and is subject to inspection by DSS.

Foreign government information must not be disclosed to nationals of a third country, including intending citizens, or to any third party, or be used for other than the purpose for which it was provided, without the prior written consent of the originating foreign government.

An export authorization is required for the export or re-export of export-controlled foreign government information except for technical data being returned to the original source of import.

Foreign government material shall be returned to the GCA or foreign government that provided the information, upon completion of the contract, unless other instructions are provided. For the destruction of TOP SECRET and SECRET foreign government information, a witness is required and destruction certificates must be retained for three years.

Our facility must promptly report to our Cognizant DSS Office, any improper transmission, loss, compromise or suspected compromise of foreign government classified information.

C. International Transfer of Classified Material

Transmission of classified material to a U.S. government activity outside of the United States will normally be through U.S. postal channels or by other means designated by the U.S. Government Contracting Agency.

All other international transfers of classified material must take place through established government- to -government channels. Normally, classified material (both U.S. and foreign) will be delivered to a designated U.S. government representative who will then transfer the material to a previously approved foreign government representative.

The FSO must be notified well in advance of a transfer of classified material to another country to ensure time to prepare for the transfer. Instructions must be prepared for all international transfers, and in some cases a Transportation Plan must be prepared and approved by the Cognizant Security Authority in advance.

D. International Visits and Control of Foreign Nationals

1. Classified Visits by Our Employees Overseas. The FSO or his/her designee will be responsible for processing all incoming and outgoing international classified visit requests. Security must be notified well in advance of an anticipated classified visit overseas. The number of days in advance the visit request must be received by the host government for NATO nations are as follows:

|  |  |  |
| --- | --- | --- |
| **Country** | **One-time and Recurring Visits** | **Amendments** |
| Belgium | 14 | 9 |
| Canada | 20 | 10 |
| Denmark | 7 | 5 |
| France | 25 | 5 |
| Germany | 25 | 10 |
| Greece | 20 | 10 |
| Italy | 14 | 7 |
| Luxembourg | 10 | 9 |
| Netherlands | 20 | 5 |
| Norway | 15 | 10 |
| Portugal | 20 | 7 |
| Spain | 25 | 8 |
| Turkey | 15 | 10 |
| United Kingdom | 21 | 5 |

The U.S. VISITS software program may be used to process international visit requests. It can be utilized to process the requests electronically and to process the requests in hard copy if we choose to do so. The software can be obtained by contacting DISCO number (614)692-2878.

Prior to traveling abroad all employees must receive a briefing on the security requirements of their assignment by the FSO or designee.

Our facility must submit a report to DISCO of the assignment of a cleared employee outside the U.S., Puerto Rico, Guam, or the Virgin Islands for a period exceeding 90 consecutive days. Our report must include:

* a local telephone and facsimile number
* complete overseas mailing address
* identity of the U.S. or foreign military installation where
* the individual(s) is assigned to include the “XX” number
* assigned by DISCO if assigned to an existing duty station.

Also, any significant change affecting the status a person’s overseas location, such as, office disestablishment, personnel change, mailing or physical address changes should be promptly reported.

To assist employees in making timely reports the following addresses and phone numbers for the Office of Industrial Security International are provided:

OISI-Europe (OISI-E)

PSC 79, Box 003

APO AE 09724

COMM: 011-322-725-0884 / FAX: 011-322-725-0116

OISI-Far East (OISI-FE)

Unit 45005

APO AP 96343-5005

COMM: 011-81-3117-63-3619

DSN: 263-3619 / FAX: 011-81-3117-63-3622

OISI-Central and South America (OISI-CASA)

c/o DSS, Industrial Security FO (S41ME)

1600 Sarno Road, Suite 201

Melbourne, FL. 32935-4992

COMM: (407)255-5185 / FAX: (407)255-5192

2. Access by Our Employees Assigned Outside of the United States

Our employees assigned outside the U.S., its possessions or territories may have access to classified information in connection with performance on a specified U.S., NATO, or foreign government classified contract. The storage of classified information by our employees at any location abroad that is not under U.S. Government control is prohibited. The storage may be at a U.S. military facility, a U.S. embassy or Consulate, or other location occupied by a U.S. Government organization.

Any of our employees assigned to foreign government or foreign contractor facilities under a direct commercial sales arrangement will be subject to the host-nation’s industrial security policies.

3. Classified Visits to Our Facility by Foreign Nationals

Our visitor record must clearly identify all foreign national visitors to this facility.

Requests for visits by foreign nationals to our facility that will involve disclosure of (1) U.S. classified information, (2) Unclassified information related to a U.S. government classified program, or (3) Plant visits covered by Section 125.5 of the ITAR, shall be processed through the sponsoring foreign government (normally the visitor’s embassy) to the U.S. government agency for approval. A visit authorization for a visit to a parent facility also may be used for visits to other divisions or subsidiaries of the same company provided disclosures are for the same purpose, the information to be disclosed does not exceed the parameters of the approved visit request, and the U.S. government agency concurs.

All foreign nationals visiting our facility must be excluded from access to all classified information and unclassified export-controlled information except as authorized by an export license, approved visit request, or other exemption to the licensing requirements. A foreign visitor should not be advised of the scope of access authorized or of limitations on access imposed by our government. Foreign visitors are never given custody of classified material except when they are acting as an official courier of their government and the Cognizant Security Authority authorizes it.

The FSO must be notified first and as soon as a possible when it is anticipated that foreign nationals will require assignment or long-term visitation in our facility.

4. Office of Industrial Security International (OISI)

To assist U.S. industry in their marketing, liaison, and technical assistance activities overseas, the Department of Defense has established the Office of Industrial Security, International (OISI). The OISI is a field extension of the Office of Industrial Security, Headquarters, DSS, and functions under its operational and administrative control. The OISI acts as the central file for information pertaining to security clearances and security assurances. Information from the files is available for official use of agencies and activities of the U.S. Government, foreign governments, NATO and U.S. contractors. OISI will conduct inspections of contractor operations on U.S. installations outside the U.S. when authorized by the Director for Industrial Security, HQ DSS. The OISI will also assist U.S. industry by:

* Arranging classified visits for U.S. contractors or their employees.
* Providing a repository for classified material.
* Providing mail channels for transmittal of classified information between a contractor in the U.S. and an approved destination outside the U.S.
* Providing security briefings and security certificates as appropriate.
* Providing advice, guidance, and assistance on security matters such as visits to military activities or contractors outside the U.S.

OISI Addresses and Phone Numbers are provided in Appendix E.

SECTION 18

## EMERGENCY PROCEDURES

Every cleared employee of this facility must be fully prepared to take the prescribed actions below in the event of disaster, civil disturbance, hostile action or any other event that may jeopardize our ability to safeguard classified material. All security personnel must thoroughly familiar with the emergency plan. The safety and health of an individual is paramount and should not be sacrificed to protect classified holdings.

Responsibilities of the Facility Security Officer

* Protect any document control records to facilitate a post emergency inventory.
* Protect classified combination records.
* Have a record of the locations of classified information by storage container and closed area.
* Provide for the safeguarding of classified information if emergency personnel, firemen, etc. must be admitted into the building(s).
* If necessary, direct the packing, loading, and transportation of classified material.

Responsibilities of All Employees

* Every precaution should be taken to protect classified material from unauthorized disclosure.
* Evaluate the situation at hand, to determine what actions should be taken initially to secure classified material, i.e., lock areas or containers, declassify computer systems, take material to the security office, etc. If classified material cannot be secured, when possible ensure a cleared guard or cleared employee remains with the material to control access to it. If there is a relatively small amount of classified material and the situation warrants it, the material may be removed from the facility by a cleared employee in coordination with the FSO and DSS.
* If possible contact the FSO, or if he/she cannot be contacted an alternate or security department representative. If no company security personnel can be contacted call the local DSS representative at.

***If necessary call the appropriate civil agencies, local or state law enforcement agencies.***

# SECTION 19

## SAMPLE SECURITY FORMS

SAMPLE ONE

*(On Company Letterhead)*

**VISIT AUTHORIZATION LETTER**

IDENTITY OF COGNIZANT SECURITY OFFICE:

FACILITY CLEARANCE LEVEL:

CAGE CODE:

NAME OF FACILITY SECURITY OFFICER:

PHONE NUMBER:

TO: Name and address of company to be visited

ATTN: Security Officer

Authorization is requested for the following personnel of this company to make a classified visit to your facility. All of the personnel listed below are U.S. citizens. Unless notified to the contrary, we will assume this request has been approved.

VISITORS DATE & PLACE OF BIRTH CLEARANCE LEVEL

[Name: Last, First, MI]

[Position or Job Title]

DATES OF VISIT: (DD/MM/YEAR) – (DD/MM/YEAR)

PERSON TO BE VISITED: [Name and Title of person to be contacted]

PURPOSE OF VISIT: [Contract number or Project]

SIGNATURE OF FSO: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SAMPLE TWO

*(On Company Letterhead)*

**CANCELLATION OF VISIT AUTHORIZATION LETTER**

TO: DATE:

ATTN: SECURITY OFFICER

REF: CONTRACT # OR PROJECT

In accordance with the provisions of the National Industrial Security Program Operating Manual, we request cancellation of the following personnel’s visit authorization letter:

NAME OF EMPLOYEE(s):

CLEARANCE LEVEL:

DATE AND PLACE OF BIRTH:

VAL REQUEST DATE:

This cancellation is assumed accomplished unless we are advised otherwise.

Sincerely,

Facility Security Officer\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SAMPLE THREE

**REQUEST FOR A PERSONNEL SECURITY CLEARANCE**

***(One Request Per Person)***

TO: THE FACILITY SECURITY OFFICER

EMPLOYEE REQUIRING CLEARANCE:

JOB TITLE:

CONTRACT NUMBER AND PROGRAM NAME:

JUSTIFICATION FOR CLEARANCE:

CERTIFICATION OF SUPERVISOR/PROGRAM MANAGER:

NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SIGNATURE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**For Security Office Use Only**

Request for PCL is approved not approved

Signature of FSO: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SAMPLE FOUR

*(On Company Letterhead)*

**VISITOR RECORD**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NAME | COMPANY | CITIZEN OF | CLASS.  YES/NO | TO SEE | TIME IN | TIME OUT |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |