



## **Security Practices & Procedures**

**May 2010**

## LETTER OF PROMULGATION

### TO THE EMPLOYEES OF FOREIGN DISCLOSURE & EXPORT SOLUTIONS CORPORATION

Foreign Disclosure & Export Solutions Corporation (“the company”) 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 the National Defense. Many of our programs and activities are vital parts of the Defense and Security systems of the United States.

**Both management and individual employees are responsible for properly safeguarding classified information.**

Our responsibility and obligation as an organization involved in such programs is to safeguard all information and material related to these classified programs.

This **Standard Practices and Procedures Manual (Security Practices and Procedures)** identifies and describes the responsibilities and duties that result from being a part of the nation’s defense team. Any employee having a question regarding his/her security responsibilities should contact the Facility Security Officer (FSO) of this company. All of us have an obligation to see that our security practices are consistent with the best interests of our nation’s defense program.

The FSO has the responsibility for supervising and directing security measures necessary for safeguarding classified information.

  
\_\_\_\_\_  
Jamie Mary McCloskey  
President

## Table of Contents

1	Defense Hotline .....	1
2	Definitions.....	2
3	Security Education.....	5
3.1	Initial Security Briefing .....	5
3.2	Classified Information Nondisclosure Agreement (SF312) .....	5
3.3	Refresher Briefings .....	5
3.4	NATO Briefing.....	6
3.5	Reporting of Irregularities.....	6
3.6	Debriefing .....	7
4	Individual Responsibility .....	8
5	Counterintelligence .....	9
5.1	National Security Threat List (NSTL) .....	9
5.1.1	Issue Threats .....	9
5.1.2	National Critical Technologies .....	9
5.2	What To Do If You Suspect You Are A Target .....	10
5.3	Suspected or Actual Cyber Intrusion .....	10
6	Clearance Procedures.....	12
6.1	Pre-Employment Clearance Action .....	12
6.2	Confidential, Secret, and Top Secret Clearances.....	12
6.3	Clearance Changes.....	12
6.4	Verification of U.S. Citizenship.....	13
6.5	SF-86 Terms of Use.....	13
6.6	Debriefing, Outprocessing, and Separation .....	13
7	FSO Responsibilities.....	14
7.1	General.....	14
7.2	Annual Inventory and Retention of Classified Material .....	14
8	Storage of Classified Material .....	16
8.1	General.....	16
8.2	End of Day Security Checks .....	16
8.3	Perimeter Control and Signage .....	16
8.4	Safeguarding of Classified Material In The Event of an Emergency .....	16
8.5	Storage Container Combination Lock Changes.....	16
9	Classified Material Markings.....	18
9.1	General.....	18
9.2	Responsible Preparation of Material Markings .....	18
9.3	Document Markings.....	18
9.4	Markings for Derivatively Classified Documents. ....	19
10	Transmission of Classified Material .....	21
10.1	Preparation and Receipting .....	21
10.2	Couriers and Handcarriers .....	21
10.2.1	Handcarriers.....	21
10.2.2	Couriers.....	21
10.3	Transmission Of Classified Information From Or To A Foreign Entity .....	22
10.4	Transmission of Classified Information Within The United States.....	22

10.5	Control Of Incoming Classified Material .....	23
10.6	Classified Meetings.....	23
11	Reproduction Of Classified Material .....	25
12	Classification And Origination Of Classified Material .....	26
12.1	Classification Of Material.....	26
12.2	Origination Of Classified Material .....	26
13	Disposition Of Classified Material .....	27
13.1	Witnesses .....	27
Attachment 1	Initial Security Briefing.....	28
Attachment 2	NATO Briefing .....	29
Attachment 3	Courier Letter .....	30
Attachment 4	Suspicious Contacts Report.....	31

# **1 Defense Hotline**

The Department of Defense provides a Defense Hotline for DoD personnel and contractor employees to allow an unconstrained avenue for reporting, without fear of reprisal, known or suspected instances of security irregularities and infractions concerning defense affiliated contracts, programs or projects, as well as fraud, waste, and abuse.

The Defense Hotline does not supplant contractor responsibility to facilitate reporting and timely investigation of security matters concerning its operation or personnel, and contractor personnel are encouraged to furnish information through established company channels. However, the Hotline may be used as an alternate means to report this type of information when considered prudent or necessary.

The Hotline is organized and administered by the Office of the Inspector General, DoD. The office initiates investigative action regarding information received through the Hotline system and has primary responsibility for ensuring the confidentiality of all system users.

This facility will conspicuously post information regarding the Defense Hotline and shall inform all employees that the Hotline may be used, if necessary, for reporting matters of national security significance, as well as fraud, waste, and abuse.

The hotline address and telephone number is as follows:

Defense Hotline  
The Pentagon  
Washington, DC 20301-1900  
800-424-9098  
703-604-8569

## 2 Definitions

**ACCESS** — The ability and opportunity to obtain knowledge of classified information. NOTE: A person may have access to classified information by being in an area where such information is kept if security measures cannot be taken to prevent the person from gaining knowledge of the classified information.

**ADVERSE INFORMATION** — Any information that adversely reflects on the integrity or character of a cleared employee, which suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security.

**AUTHORIZED PERSON** — A person who has a need-to-know for classified information in the performance of official duties and who has been granted personnel clearance at the required level.

**CLASSIFICATION AUTHORITY** — The authority that is vested in a government official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

**CLASSIFIED CONTRACT** — Any contract that requires or will require access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.)

**CLASSIFICATION GUIDE** — A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specific information to be classified on a derivative basis. NOTE: Classification guides are generally provided to contractors via the DD Form 254).

**CLASSIFIED INFORMATION** — See “National Security Information.”

**COGNIZANT SECURITY OFFICE** — The office of the DIS Director of Industrial Security that has industrial security jurisdiction over the geographical area in which a contractor is located. For most purposes, the Field Office handles all concerns of the contractor.

**COMPROMISE** — The disclosure of classified information to persons not authorized access to it.

**CONFIDENTIAL** — “Confidential” is the designation that shall be applied to information or material the unauthorized disclosure of which could be reasonably expected to cause damage to the national security.

**DOCUMENT** — Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards, tapes, charts, maps, paintings, drawings, engravings, sketches, working notes and papers; reproductions of

such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.

**FACILITY** — A plant, lab, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, which, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined above.)

**FACILITY CLEARANCE** — An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

**FOREIGN INTEREST** — Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized under the laws of any country other than the US or its possessions, and any person who is not a citizen or national of the US.

**FOREIGN NATIONALS** — Persons not citizens or nationals of the US.

**HOME OFFICE FACILITY** — The headquarters facility of a multiple facility organization.

**LETTER OF CONSENT** — (DISCO FORM 560) The form used by DISCO to notify a contractor that a PCL or a Limited Access Authorization has been granted to an employee.

**MULTIPLE FACILITY ORGANIZATION** — A legal entity that is composed of two or more entities.

**NEED-TO-KNOW** — A determination made by the possessor of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a classified contract or program approved by a User Agency.

**OFFICERS** — Those persons in positions established as officers in the articles of incorporation or bylaws of the organization. This definition includes all principal officers; that is, those persons occupying a position normally identified as president, senior vice president, secretary, treasurer, and those persons occupying similar positions. In unusual cases, the determination of principal officer status may require a careful analysis of an individual's assigned duties, responsibility, and authority as officially recorded by the organization. Excluded from this definition are: (i) assistant vice presidents who have no management responsibilities related to performance on classified contracts, (ii) assistant secretaries, and (iii) assistant treasurers.

**PARENT** — A corporation that can control another corporation (subsidiary) by ownership of a majority of its stock. The control may exist by direct stock ownership of an immediate subsidiary or by indirect ownership through one or more intermediate levels of subsidiaries.

**PERSONNEL SECURITY CLEARANCE** — An administrative determination that an

individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

**REPRESENTATIVE OF A FOREIGN INTEREST (RFI)** — A citizen or national of the US, or intending citizen to the US who is acting as a representative of a foreign interest.

**SECRET** — The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

**SUBSIDIARY** — A corporation that is controlled by another corporation (parent) by reason of the latter corporation's ownership of at least a majority (over 50%) of the capital stock. A subsidiary is a legal entity and shall be processed separately for an FCL.

**TOP SECRET** — The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

**UNAUTHORIZED PERSON** — A person not authorized to have access to specific classified information in accordance with the requirements of the National Industrial Security Program Operating Manual.

### **3 Security Education**

Individuals who are authorized access to classified information are important targets for hostile intelligence services. It is common practice for hostile intelligence services to establish and maintain dossiers on personnel of intelligence interest, particularly of personnel whose jobs afford them access to either classified information or technology-controlled information. These services are constantly on the alert for opportunities to gain any kind of advantage that can be exploited. If there are any questions about what is necessary to avoid these services, consult with the FSO.

The FSO shall ensure that the following briefings are provided to all cleared employees as necessary:

#### **3.1 Initial Security Briefing**

Prior to being granted access to classified information, an employee shall receive an initial security briefing that includes the following:

- a. A threat awareness briefing.
- b. A defensive security briefing.
- c. An overview of the security classification system.
- d. Employee reporting obligations and requirements.
- e. Security procedures and duties applicable to the employee's job.

A copy of the Initial Security Briefing is attached to this SSP as Attachment 1.

#### **3.2 Classified Information Nondisclosure Agreement (SF312)**

Legal and binding agreement between the US Government and an individual who is cleared for access to classified information. This briefing is required and must be signed prior to an individual may have access to classified information. Any refusal to sign/execute the SF-312 will be reported to DISCO.

#### **3.3 Refresher Briefings**

Remind cleared employees of their obligation to protect classified information and responsibilities regarding disclosure to authorized individuals.

### **3.4 NATO Briefing**

FDE Solutions Corp. employees with a security clearance of SECRET (or higher) shall have an annual NATO security refresher briefing as part of their annual training requirements.

Before having access to NATO classified information, employees shall be given a NATO security briefing that covers the requirements of Section 10-7 of the NISPOM and the consequences of negligent handling of NATO classified information. When access to NATO classified information is no longer required, the employee shall be debriefed. The employee shall sign a certificate stating that they have been briefed or debriefed, as applicable, and acknowledge their responsibility for safeguarding NATO information.

Certificates shall be maintained for 2 years for NATO SECRET and CONFIDENTIAL, and 3 years for COSMIC TOP SECRET and all ATOMAL information.

The FSO shall maintain a record of all NATO briefings and debriefings in the Cognizant Security Agency (DSS)-designated database.

The FSO shall be initially briefed by a representative of the Cognizant Security Agency (DSS).

### **3.5 Reporting of Irregularities**

Personnel, whether cleared or uncleared, that work for FDE Solutions Corp. are required to report certain events that have an impact on the status of the facility clearance (FCL), that impact on the status of an employee's personnel security clearance (PCL), that affect proper safeguarding of classified information, or that indicate classified information has been lost or compromised. The FSO will use the annual training program to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the FSO, the Federal Bureau of Investigation (FBI), or other Federal authorities as required by the NISPOM, the terms of a classified contract, and U.S. law. The FSO or reporting person shall provide complete information to enable the Cognizant Security Agency (DSS) to ascertain whether classified information is adequately protected. The FSO shall submit reports to the FBI and to their Cognizant Security Agency (DSS) as specified in this section.

a. When the reports are classified or offered in confidence and so marked by the contractor, the information will be reviewed by the Cognizant Security Agency (DSS) to determine whether it may be withheld from public disclosure under applicable exemptions of the Freedom of Information Act (5 U.S.C. 552)).

b. When the reports are unclassified and contain information pertaining to an individual, the Privacy Act of 1974 (5 U.S.C. 552a)) permits withholding of that information from the individual only to the extent that the disclosure of the information would reveal the identity of a source who furnished the information to the U.S. Government under an expressed promise that

the identity of the source would be held in confidence. The fact that a report is submitted in confidence must be clearly marked on the report.

c. The FSO shall promptly submit a written report to the nearest field office of the FBI regarding information coming to the FSO's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations. An initial report may be made by phone, but it must be followed in writing, regardless of the disposition made of the report by the FBI. A copy of the written report shall be provided to the Cognizant Security Agency (DSS).

### **3.6 Debriefing**

Contractors shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's PCL is terminated, suspended, or revoked; and upon termination of the FCL.

## 4 Individual Responsibility

Each cleared employee of this company is required to report to the FSO any of the following:

- ESPIONAGE — Information concerning existing or threatened espionage, sabotage, or subversive activities. The FSO will forward a report to the Fill and the Cognizant Security Agency (DSS).
- COMPROMISE — The loss, compromise, or suspected compromise of classified information as well as failures to comply with the NISPOM.
- ADVERSE INFORMATION — Information regarding a cleared employee or employee in process for a clearance which suggests that his/her ability to safeguard classified information may be impaired. Examples of adverse information include criminal activities, treatment for mental/emotional disorders, excessive use of intoxicants, use of illegal, controlled substances, excessive indebtedness or financial difficulties.
- SECURITY VIOLATIONS — Should be reported as adverse information if a culpable individual can be determined. The following is a suggested scale of disciplinary action for those individuals determined to be culpable for a security violation.
  - 1st Violation within a 12-month consecutive period — Written reprimand
  - 2nd violation within a 12-month consecutive period — Written reprimand and other corrective action deemed appropriate
  - 3rd violation within a 12-month consecutive period — Written reprimand and other action deemed appropriate as applicable by the FSO and supervisor based upon the current and past violation.
- NAME CHANGE/CITIZENSHIP — Change in legal name or citizenship.
- REPRESENTATIVE OF A FOREIGN INTEREST (RFI) — Cleared employee who becomes an RFI or whose status as an RFI has changed.

These examples are not all-inclusive. Please refer additional questions to the FSO for determination. Reporting of adverse information does not necessarily mean the termination of a personnel clearance. This company has established a system for reporting adverse information, which includes cleared supervisors and managerial personnel playing an active role in identifying and reporting such information to the FSO.

## **5 Counterintelligence**

### **5.1 National Security Threat List (NSTL)**

We live in a world of rapid change. In recent years, there have been marked shifts in the area of international relations. Reflecting these shifts, there has been rearticulating of US Foreign CI strategy known as the NSTL. The NSTL combines two elements. First, it includes national security issues that 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 US security interest.

The issue threat portion of the NSTL was developed by the US Intelligence Community and key elements of the US Government. Seven categories of foreign intelligence activity were deemed to be significant threats to US national security interests.

#### **5.1.1 Issue Threats**

Foreign Intelligence Activities involving:

- 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 establishment and related activities of national preparedness.
- US critical technologies as identified by the National Critical Technologies Panel.
- Targeting of US Intelligence and foreign affairs information and US Government officials.
- Collection of US Industrial proprietary economic information and technology, the loss of which would undermine the US strategic industrial position.
- Clandestine foreign intelligence activity in the US.
- Perception management and Active activities.

#### **5.1.2 National Critical Technologies**

The following have been identified as such:

- MATERIALS — Materials synthesis and processing, electronic and photogenic materials, ceramics, composites or high-performance metals and alloys
- MANUFACTURING — Flexible computer-integrated manufacturing, intelligence processing equipment, micro- and nanofabrication, or systems management technologies
- INFORMATION AND COMMUNICATIONS - Software, high-performance computing and networking, micro- and opto-electronics, high-definition imaging and

displays, sensors and signal processing, data storage and peripherals or computer simulation and modeling

- BIOTECHNOLOGY AND LIFE SCIENCES — Applied molecular biology or Medical technology
- AERONAUTICS AND SURFACE TRANSPORTATION - Aeronautics or surface transportation technologies
- ENERGY AND ENVIRONMENT — Energy technologies, pollution minimization, remediation, and waste management

## **5.2 What To Do If You Suspect You Are A Target**

You may be the target of foreign intelligence activities if you or FDE Solutions Corp. is associated with one or more of the critical technologies. Overseas travel, foreign contact, and joint ventures may further increase your company's exposure to the efforts of foreign intelligence collectors. For this reason, DSS has established a Counterintelligence Office and all issues may be addressed to the DSS field office via the FSO.

FDE Solutions Corp. employees may find a suspicious contacts reporting form on the company's website under the "Employees Only" link found on the [www.fdesolutions.com](http://www.fdesolutions.com) home page.

## **5.3 Suspected or Actual Cyber Intrusion**

Paragraph 1-301 of the NISPOM requires FDE Solutions Corp. to promptly report to the Federal Bureau of Investigation (FBI) (with a copy to DSS) information coming to the company's attention concerning "actual, probable or possible espionage, sabotage, terrorism, or subversive activities" at any of the contractor's locations.

Certain cyber intrusions will fall under the reporting requirement of NISPOM 1-301, regardless of the classification level of information contained on the affected system. Specifically, cyber intrusions that indicate actual, probable or possible espionage, sabotage, terrorism, or subversive activities against information systems (IS) maintained by FDE Solutions Corp. must be reported to the FBI, with a copy to DSS, regardless of whether the IS processes classified or unclassified information.

Cyber intrusions are often targeted against specific information or technologies; however, the target cannot always be easily identified at the time the intrusions take place. It may be unclear that the intrusions are intended to lead to espionage, sabotage, terrorism, or subversive activities when the initial intrusions concern systems processing only unclassified information. Data gleaned from intrusions of systems containing unclassified information can include the identity of systems administrators, personal identifying information of employees that may provide indicators of exploitable issues (e.g., financial problems, drug use, etc.), or system vulnerabilities. This data can then be used advantageously for nefarious reasons and to focus more specific technical and non-technical exploitation techniques. These intrusions may signal

an increased level of security risk to the contractor, the classified Government programs it supports, the information it holds, and the company's employees.

A cyber intrusion reportable under NISPOM 1-301 may involve one or more of a combination of active efforts, such as: port and services scanning from consistent or constant addresses, hacking into the system, placing malware hacking tools into the system, or passive efforts (e.g., unsolicited emails containing malware or internet sites that entice users to download files that contain embedded malware). Reportable cyber intrusions may include exploitation of knowledgeable persons through "phishing" and "social engineering" that occur in or out of phase with the application of the malware.

The FDE Solutions Corp. FSO should consider the following guidelines when making a determination to report a cyber intrusion (as defined in the National Information Assurance Glossary, Committee on National Security Systems Instruction No. 4009, is the unauthorized act of bypassing the security mechanisms of a system) to the FBI and to DSS under NISPOM paragraph 1-301:

- Evidence of an advanced persistent threat;
- Evidence of unauthorized exfiltration or manipulation of information;
- Evidence of preparation of contractor systems or networks for future unauthorized exploitation;
- Activity that appears to be out of the ordinary, representing more than nuisance incidents; and
- Activities, anomalies, or intrusions that are suspicious and cannot be easily explained as innocent.

FDE Solutions Corp. personnel are also reminded that they are required by NISPOM paragraph 1-302b, to report to DSS efforts by any individual, regardless of nationality, to "obtain illegal or unauthorized" access to IS processing classified information. Additionally, under NISPOM paragraph 1-302j, the company must report "significant vulnerabilities" identified in IS "hardware and software used to protect classified material."

## **6 Clearance Procedures**

### **6.1 Pre-Employment Clearance Action**

If access to classified information is required by a potential employee immediately upon commencement of their employment, a PCL application may be submitted to the Cognizant Security Agency (DSS) by the contractor prior to the date of employment provided a written commitment for employment has been made by the contractor, and the candidate has accepted the offer in writing. The commitment for employment will indicate that employment shall commence within 30 days of the granting of eligibility for a PCL.

### **6.2 Confidential, Secret, and Top Secret Clearances**

Initial applications for clearances will be submitted as follows:

- CONFIDENTIAL-SF 86, FD 258 (Fingerprint Card)
- SECRET-SF 86, FD 258 (Fingerprint Card)
- TOP SECRET-SF 86, DD Form 1879, FD 258 (Fingerprint Card)

Clearance applications may be submitted via mail or electronically (EPSQ). For further information on the EPSQ, the FSO may contact the DSS field office.

Generally and unless otherwise stated, all levels of investigations will cover a 7 year investigative scope.

### **6.3 Clearance Changes**

DISCO Form 562, "Personnel Security Clearance Change Notification," will be utilized to report changes concerning any clearance issued or being processed by DISCO:

- Termination of employment
- MFO transfers
- Downgrading
- Reinstatements, concurrent & conversions
- Administrative termination of clearance
- Name change
- Change in employment status (from employee to KMP or KMP to employee)
- Naturalization

## **6.4 Verification of U.S. Citizenship**

FDE Solutions Corporation will require each applicant for a PCL who claims U.S. Citizenship to produce evidence of citizenship. Documents acceptable for proof of citizenship are listed in 2-207 of the NISPOM.

## **6.5 SF-86 Terms of Use**

The FSO shall inform the employee that the SF 86 is subject to review and shall review the application solely to determine its adequacy and to ensure that necessary information has not been omitted. The FSO or designee shall provide the employee with written notification that review of the information is for adequacy and completeness, information will be used for no other purpose within the company, and that the information provided by the employee is protected by the Privacy Act of 1975. The FSO or designee shall not share information from the employee's SF 86 within the company and shall not use the information for any purpose other than determining the adequacy and completeness of the SF 86.

## **6.6 Debriefing, Outprocessing, and Separation**

The FDE Solutions Corp FSO or designated representatives shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's PCL is terminated, suspended, or revoked; and upon termination of the company's Facility Clearance.

The FSO or designated representative shall also obtain the outbriefed person's signature on the SF-312 (to be forwarded to DISCO); remove access from the JPAS record for FDE Solutions Corp.; and remove the person from the company's JPAS PSM Net.

## **7 FSO Responsibilities**

### **7.1 General**

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

- To receive, prepare, and submit reports such as changed conditions, upgrades and downgrades, name changes, address changes, corporate officer changes, terminations, ownership changes etc.
- To maintain all personnel security clearance records, to include “Letter of Notification of Security Clearance” (381-R), “Department of Defense Security Agreement” (UD Form 441 and 441-1), and “Certificate Pertaining to Foreign Interests” (SF 328).
- To maintain all personnel security clearance records such as the “Letter of Consent” (DISCO Form 560), “Classified Information Nondisclosure Agreement” (SF 312), “Personnel Security Clearance Change Notification” (DISCO Form 562), and copies of all clearance paperwork.
- To maintain the NISPOM, as well as to prepare, maintain, and distribute this Standard Practice Procedure (Security Practices and Procedures) as required by the Cognizant Security Agency (DSS), to implement within the company the applicable requirements of the NISPOM, and to revise the Security Practices and Procedures as necessary
- To brief all cleared employees as necessary and to execute the SF 312 prior to classified access
- To process all clearance requests for CONFIDENTIAL, SECRET AND TOP SECRET
- To conduct self-inspections on a continuing basis at intervals consistent with risk management principals.

### **7.2 Annual Inventory and Retention of Classified Material**

The FSO shall conduct an annual inventory of FDE Solutions Corp.’s classified holdings. All holdings that go beyond the storage time periods allowed in the NISPOM or the DD254, whichever is shorter, will be destroyed.

Per the NISPOM, paragraph 5-701, FDE Solutions Corp. is authorized to retain classified material received or generated under a contract for a period of 2 years after completion of the contract, provided the Government Contracting Authority does not advise to the contrary. If retention is required beyond the 2-year period, the FSO must request and receive written retention authority from the Government Contracting Authority.

- a. Contractors shall identify classified material for retention beyond 2 years as follows:

(1) TOP SECRET material shall be identified in a list of specific documents unless the Government Contracting Authority authorizes identification by subject matter and approximate number of documents.

(2) SECRET and CONFIDENTIAL material may be identified by general subject matter and the approximate number of documents.

b. Contractors shall include a statement of justification for retention based on the following:

(1) The material is necessary for the maintenance of the contractor's essential records.

(2) The material is patentable or proprietary data to which the contractor has title.

(3) The material will assist the contractor in independent research and development efforts.

(4) The material will benefit the U.S. Government in the performance of other prospective or existing agency contracts.

(5) The material will benefit the U.S. Government in the performance of another active contract and will be transferred to that contract (specify contract).

c. If retention beyond 2 years is not authorized, all classified material received or generated in the performance of a classified contract shall be destroyed unless it has been declassified or the Government Contracting Authority has requested that the material be returned.

## **8 Storage of Classified Material**

### **8.1 General**

FDE Solutions Corp. personnel shall be responsible for safeguarding classified information in their custody or under their control. Individuals are responsible for safeguarding classified information entrusted to them. The extent of protection afforded classified information shall be sufficient to reasonably foreclose the possibility of its loss or compromise.

### **8.2 End of Day Security Checks**

The last FDE Solutions Corp. person with a security clearance to leave the office each day shall verify that all classified material and security repositories have been appropriately secured.

### **8.3 Perimeter Control and Signage**

FDE Solutions Corp.'s classified material shall only be used in areas as designated by the FSO. Signs that warn persons entering the FDE Solutions Corp. residence that anyone entering or departing these areas may be subject to an inspection of their personal effects, regardless of whether suspicion of illegal activity is suspected or not, shall not be posted or required as indicated in NISPOM 5-103a.

Only cleared FDE Solutions Corp. personnel shall enter the classified perimeter when the storage container is open.

### **8.4 Safeguarding of Classified Material In The Event of an Emergency**

In the event of an emergency of any sort, cleared FDE Solutions Corp. personnel working on classified material shall immediately return the material to the approved storage container and lock the container prior to departing the area. If the emergency results in rendering the facility incapable of continuing to store classified material, the FSO shall immediately report this fact to the company's DSS representative and the Cognizant Security Agency (DSS).

### **8.5 Storage Container Combination Lock Changes**

Combinations shall be changed by a person authorized access to the contents of the container, or by the FSO or his or her designee. Combinations shall be changed as follows:

- a. The initial use of an approved container or lock for the protection of classified material.
- b. The termination of employment of any person having knowledge of the combination, or when the clearance granted to any such person has been with-drawn, suspended, or revoked.
- c. The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended.
- d. At other times when considered necessary by the FSO or Cognizant Security Agency (DSS).

## **9 Classified Material Markings**

### **9.1 General**

Physically marking classified information with appropriate classification markings serves to warn and inform holders of the information of the degree of protection required. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. Therefore, it is essential that all classified information and material be marked to clearly convey to the holder the level of classification assigned, the portions that contain or reveal classified information, the period of time protection is required, and any other notations required for protection of the information.

As a general rule, the markings specified in NISPOM paragraphs 4-202 through 4-208 are required for all classified information regardless of the form in which it appears. Some material, such as documents, letters, and reports, can be easily marked with the required markings. Marking other material, such as equipment, IS media, and slides may be more difficult due to size or other physical characteristics. Since the primary purpose of the markings is to alert the holder that the information requires special protection, it is essential that all classified material be marked to the fullest extent possible to ensure the necessary safeguarding.

### **9.2 Responsible Preparation of Material Markings**

All classified material shall be marked to show the name and address of the FDE Solutions Corp. person responsible for its preparation, and the date of preparation. These markings are required on the face of all classified documents.

The highest level of classified information contained in a document is its overall marking. The overall marking shall be conspicuously marked or stamped at the top and bottom on the outside of the front cover, on the title page, on the first page, and on the outside of the back. All copies of classified documents shall also bear the required markings. Overall 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 markings shall be furnished to recipients.

### **9.3 Document 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 the portion is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contain or reveal classified information. 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, (C) for CONFIDENTIAL, and (U) for UNCLASSIFIED shall be used.

a. Illustrations, photographs, figures, graphs, drawings, charts, or similar portions contained in classified documents shall be marked clearly to show their classified or unclassified status. These classification markings shall not be abbreviated and shall be prominent and placed within or contiguous to such a portion. Captions of such portions shall be marked on the basis of their content.

b. If, in an exceptional situation, marking of the portions 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.

Unclassified subjects and titles shall be selected for classified documents, if possible. A classified subject or title shall be marked with the appropriate symbol placed immediately following the item.

#### **9.4 Markings for Derivatively Classified Documents.**

All classified information shall be marked to reflect the source of the classification and declassification instructions. Documents shall show the required information either on the cover, first page, title page, or in another prominent position. Other material shall show the required information on the material itself or, if not practical, in related or accompanying documentation.

a. "DERIVED FROM" Line. The purpose of the "Derived From" line is to link the derivative classification applied to the material by the contractor and the source document(s) or classification guide(s) under which it was classified. In completing the "Derived From" line, the contractor shall identify the applicable guidance that authorizes the classification of the material. Normally this will be a security classification guide listed on the Contract Security Classification Specification or a source document. When identifying a classification guide on the "Derived From" line, the guide's title or number, issuing agency, and date shall be included. Many Contract Security Classification Specifications cite more than one classification guide and/or the contractor is extracting information from more than one classified source document. In these cases, the contractor may use the phrase "multiple sources." When the phrase "multiple sources" is used, the contractor shall maintain records that support the classification for the duration of the contract under which the material was created. These records may take the form of a bibliography identifying the applicable classification sources and be included in the text of the document or they may be maintained with the file or record copy of the document. When practical, this information should be included in or with all copies of the derivatively classified document. If the only source for the derivative classification instructions is the Contract Security Classification Specification, the date of the specification and the specific contract number for which it was issued shall be included on the "Derived From" line.

b. "DECLASSIFY ON" Line. The purpose of the "Declassify On" line is to provide declassification instructions appropriate for the material. When completing this line, the FDE Solutions Corp. personnel shall use the information specified in the Contract Security Classification Specification or classification guide furnished with a classified contract. Or, the document shall carry forward the duration instruction from the source document or classification guide (e.g., date or event). When the source is marked "Original Agency's Determination Required" (OADR) or "X1 through X8", the "Declassify On" line should indicate that the source material was marked with one of these instructions and the date of origin of the most recent source document as appropriate to the circumstances. When a document is classified derivatively on the basis of more than one source document or more than one element of a classification guide, the "Declassify On" line shall reflect the longest duration of any of its sources. Material containing RD or FRD shall not have a "Declassify On" line.

c. "DOWNGRADE TO" Line. When downgrading instructions are contained in the Contract Security Classification Specification, classification guide or source document a "Downgrade To" line will be included. When completing this line, the contractor shall insert SECRET or CONFIDENTIAL and an effective date or event. The markings used to show this information are:

DERIVED FROM  
DOWNGRADE TO ON  
DECLASSIFY ON

d. "CLASSIFIED BY" Line and "REASON CLASSIFIED" Line. As a general rule, a "Classified By" line and a "Reason Classified" line will be shown only on originally classified documents. However, certain agencies may require that derivatively classified documents contain a "Classified By" line to identify the derivative classifier and a "Reason Classified" Line to identify the specific reason for the derivative classification. Instructions for the use of these lines will be included in the security classification guidance provided with the contract.

## **10 Transmission of Classified Material**

### ***10.1 Preparation and Receipting***

Classified information to be transmitted outside of a facility will be enclosed in opaque inner and outer covers. The inner cover will be a sealed wrapper or envelop plainly marked with the assigned classification and addresses of both the sender and addressee. The outer cover will be sealed and addressed with no identification of the classification of its contents. A receipt will be attached to or enclosed in the inner cover. The receipt will identify the sender, the addressee and the document, but shall contain no classified information. It will be signed by the recipient, returned to the sender and retained for 2 years.

### ***10.2 Couriers and Handcarriers***

The following procedures will apply when transmitting classified information by use of a handcarrier or courier.

#### **10.2.1 Handcarriers**

Handcarriers will be used when there is no other method by which to transfer the information. A handcarrier is an employee who occupies activities other than simply handcarrying classified information.

#### **10.2.2 Couriers**

A courier is an employee whose sole responsibility is serving as a handcarrier. This individual is designated as an official courier. The following procedures will apply:

- FSO will obtain FCL and storage verification of the receiving site.
- The courier's clearance will be forwarded to the receiving site.
- The courier will be briefed on his/her responsibilities and provided with an identification card (Attachment 3).
- Classified material will be packaged for transmission and will remain in the possession of the courier at all times.

### **10.3 Transmission Of Classified Information From Or To A Foreign Entity**

The DSS Field Office will be contacted immediately for these transmissions, as they must occur government-to-government.

### **10.4. Transmission of Classified Information Within The United States**

SECRET material may be transmitted by one of the following methods within and directly between the United States and its territorial areas:

- a. 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.
- b. A cleared commercial carrier.
- c. A cleared commercial messenger service engaged in the intracity/local area delivery (same day delivery only) of classified material.
- d. A commercial delivery company, approved by the Cognizant Security Agency (DSS), that provides nation-wide, overnight service with computer tracking and reporting features. Such companies need not be security cleared. This is the preferred method of transmission for FDE Solutions Corp. The FDE Solutions Corp. preferred commercial delivery company is Federal Express (FedEx).
- e. Other methods as directed in writing by the Government Contracting Authority.

For transmission of classified information to U.S. representatives outside of the United States and its territories, see the FDE Solutions Corp. FSO for an approved method of transmission.

Transmission Method	Classification Level		
	Top Secret	Secret	Confidential
Defense Courier Service	X	X	X
Designated courier, handcarrier, or escort	X	X	X
CSA-approved secure communications	X	X	X
USPS Express Mail		X	X
USPS Registered Mail		X	X
Cleared commercial carrier		X	X
Cleared commercial messenger service		X	X
CSA-approved commercial delivery company		X	X
Other methods approved by GCA		X	X
USPS Certified Mail			X
Non-cleared commercial carriers			X

## **10.5 Control Of Incoming Classified Material**

In order to ensure the proper safeguarding of classified material, the following procedures are required:

The receipt and dispatch records will be maintained of all SECRET and CONFIDENTIAL information and will include:

- Date of the document
- Activity from which the document was received
- Date of the receipt
- Classification
- Unclassified title
- Disposition of material and date
- Date by which destruction must be performed

Accountability records will be maintained for all classified information received or generated by the company.

All classified material will be received by cleared individuals. In effect, all FDE Solutions Corp. personnel who handle US registered, US express, or certified will be appropriately cleared. Non-cleared individuals shall be instructed not to sign for or handle these types of mail deliveries.

## **10.6 Classified Meetings**

FDE Solutions Corp. personnel desiring to conduct meetings requiring government sponsorship shall submit their requests to the Government Agency having principal interest in the subject matter of each meeting. The request for authorization shall include the following information:

(1) An explanation of the government purpose to be served by disclosing classified information at the meeting and why the use of conventional channels for release of the information will not advance those interests.

(2) The subject of the meeting and scope of classified topics, to include the classification level, to be disclosed at the meeting.

(3) The expected dates and location of the meeting.

(4) The general content of the proposed announcement and/or invitation to be sent to prospective attendees or participants.

(5) The identity of any other non-government organization involved and a full description of the type of support it will provide.

(6) A list of any foreign representatives (including their nationality, name, organizational affiliation) whose attendance at the meeting is proposed.

(7) A description of the security arrangements necessary for the meeting to comply with the requirements of this manual.

## **11 Reproduction Of Classified Material**

Classified information may be reproduced using only the flat-bed scanner and classified laptop computer approved for use in the NISP-accredited Information System.

Unless restricted by the Government Contracting Authority, SECRET and CONFIDENTIAL documents may be reproduced as follows:

- (1) Performance of a prime contract or a subcontract in furtherance of a prime contract.
- (2) Preparation of a solicited or unsolicited bid, quotation, or proposal to a Federal agency or prospective subcontractor.
- (3) Preparation of patent applications to be filed in the U.S. Patent Office.

Reproduced copies of classified documents shall be subject to the same protection as the original documents.

See Chapter 9 of this Security Practices and Procedures regarding classification markings. All reproductions of classified material shall be conspicuously marked with the same classification markings as the material being reproduced. Copies of classified material shall be reviewed after the reproduction process to ensure that these markings are visible.

## **12 Classification And Origination Of Classified Material**

### ***12.1 Classification Of Material***

It may be necessary in the performance of a contract to classify material that has been generated by the company. The following procedures will apply:

- Normally, security classification will be provided by the government customer involved with the classified contract via the DD Form 254. The company should use this classification guidance when it produces classified relative to the contract.
- Whenever the company originates information other than in the performance of a current contract, it is to be classified if the company already knows it is classified.
- If the company originates information it thinks may be classified, it will protect the information as though classified until a determination can be made by the appropriate government agency.
- The responsibility for reviewing the necessity, currency, and accuracy of the classified material lies with the supervisor/program manager on charge of the contract.

### ***12.2 Origination Of Classified Material***

When the company is involved in the generation of classified documents or material, the following procedures will apply (5-205b, NISPOM):

- Classified working papers will be dated when created; marked with overall classification, and the annotation "WORKING PAPERS."
- The markings required for finished documents are not required for working papers, but contractors are encouraged to use portion markings to the extent practical.

## **13 Disposition Of Classified Material**

The quantity of classified material on hand will be minimized to the maximum extent possible consistent with contractual performance. Once classified material has served its purpose, it will be returned to the government customer or destroyed as early as possible.

Classified documents will be destroyed in accordance 5-705 of the NISPOM.

### **13.1 Witnesses**

A witness, if available, shall oversee the destruction of classified information.

Destruction records will indicate the date and the material and be signed by both individuals involved in the destruction.

Destruction records will be maintained for two years.

**Attachment 1 Initial Security Briefing**

**Attachment 2 NATO Briefing**

**Attachment 3 Courier Letter**

**Attachment 4 Suspicious Contacts Report**