SECURITY STANDARD PRACTICES AND PROCEDURES (SPP)

Don Selvy Enterprises, Inc.
103 West Riding Drive
Bel Air, MD 21014

August 2021

Forward

Don Selvy Enterprises, Inc. (DSE) has entered into a Security Agreement with the Department of Defense 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 are responsible for properly safeguarding the classified information entrusted to our care.

Our Standard Practice Procedures (SPP) conforms to the security requirements set forth in government regulations – 32 Code of Federal Regulation (CFR) Part 117, NISPOM (National Industrial Security Program Operating Manual). The purpose of our SPP is to provide our employees with the requirements of 32 CFR Part 117 as they relate to the type of work we do. This document should also serve as an easy reference when questions about security arise.

Our company fully supports the National Industrial Security Program (NISP). All of us have an obligation to ensure that our security practices contribute to the security of our nation's classified defense information.

Don Selvy
DSE FSO and DSE President

Table of Contents

1. Introduction

This Standard Practices and Procedures (SPP) describes Don Selvy Enterprises, Inc. (DSE) policies regarding the handling and protection of classified information. This SPP is applicable to all employees, subcontractors, consultants, vendors, and visitors to our facility and is a supplement to the National Industrial Security Program Operating Manual (NISPOM)[1] policies codified in 32 Code of Federal Regulation Part 117, NISPOM, which takes precedence in instances of apparent conflict.

2. Facility Information

2.1. Facility Clearance

A facility clearance (FCL) is an administrative determination that a facility is eligible for access to classified information or award of a classified contract. DSE has a SECRET facility clearance. The FCL is valid for access to classified information at the SECRET or lower classification level.

2.2. Facility Security Officer

Having a facility clearance, DSE must agree to adhere to the rules of the National Industrial Security Program (NISP). As part of the NISP, contractors are responsible for appointing a Facility Security Officer (FSO). The FSO must be a U.S. citizen, an employee of the company, and cleared to the level of the facility clearance. The FSO must complete required training and is responsible for supervising and directing security measures necessary for implementing the NISPOM and related Federal requirements for classified information. Don Selvy is the FSO for DSE and can be reached at (410) 838-5073 or dselvy@dse-inc.net. The Assistant FSO is KC Pake. KC Pake can be reached at (410) 459-9601 or kpake@dse-inc.net.

2.3. Storage Capability

The facility clearance level is separate from the storage capability level. Contractors must receive a separate approval prior to storing any classified information. DSE is not authorized to store classified material at any level of classification. Section 9 discusses the procedures for appropriate handling, storage, and control of classified materials.

3. Personnel Security Clearances

3.1. Clearance Procedures

DSE 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 number of employees processed for a clearance will be limited to the minimum necessary for operation efficiency.

DSE will utilize the Defense Information System for Security (DISS) to initiate the clearance request process. Each applicant for a security clearance must produce evidence of citizenship such as an original birth certificate or passport. Applicants will complete the Questionnaire for National Security Positions (SF-86) through OPM's electronic questionnaires for investigation processing (e-QIP) system.

The FSO will ensure that prior to initiating the e-QIP action, the applicant is provided guidance from 32 CFR Part 117.10(d). This ensures the employee is aware that the SF-86 is subject to review by the FSO only to determine the information is adequate and complete but will be used for no other purpose and protected in accordance with the Privacy Act of 1975.

While DSE initiates the clearance process for employees, the government will make the determination of whether an individual is eligible to access classified information and grant the personnel clearance.

3.2. Reinvestigations

Depending upon the level of access required, individuals holding security clearances are subject to a periodic reinvestigation (PR) at a minimum of every five years for Top Secret, 10 years for Secret and 15 years for Confidential. Our FSO is responsible for reviewing all access records to ensure employees are submitted for PRs as required.

3.3. Continuous Evaluation

The DoD Continuous Evaluation (CE) program is an ongoing screening process to review the background of an individual who is assigned to a sensitive position or has access to classified information. CE leverages automated record checks and applies business rules (aligned to the Federal Investigative Standards) to assist in the ongoing assessment of an individual's continued eligibility.

Deferment refers to the process implemented by DoD, in July 2018, and currently being used by departments and agencies to permit the focus of investigative resources on the inventory of pending initial investigations. New reinvestigation requests are screened using a risk management-based approach, where the Standard Form 86 (SF-86) is analyzed using deferment protocol(s) and is identified for either enrollment in Continuous Evaluation (CE) or submission to an Investigation Service Provider (ISP) for a reinvestigation.

Once in CE, future investigations may be predicated on the CE deferment status. Most DSE employees can anticipate indication into the CE program. Nonetheless, submission of a SF-86 reinvestigation request is still required on the same PR schedule based upon clearance level and the most recent investigation date. DCSA will make a determination whether the SF-86 will proceed with a full investigation or if an updated clearance can be issued based on CE status.

3.4. Consultants

For security administration purposes, consultants are treated as employees of DSE and must comply with this SPP and the NISPOM. Consultants will, however, be required to execute a Consultant Agreement which outlines any security responsibilities specific to the consultant.

Note: If DSE sponsors a consultant for a PCL, DSE must compensate the consultant directly; otherwise, the company receiving compensation must obtain a Facility Security Clearance (FCL) and serve as a subcontractor to DSE.

4. Security Education

4.1. Initial Security Briefings

All cleared employees must receive an initial security briefing and sign a Nondisclosure Agreement (SF 312) prior to being granted access to classified material for the first time. The SF 312 is an agreement

between the United States and a cleared individual. At a minimum, the initial briefing will include the following:

- Threat Awareness Briefing
- Defensive Security Briefing
- Overview of Security Classification System
- Employee reporting obligations and requirements
- Overview of the SPP

4.2. Annual Security Briefings

Annual briefings will be provided to all cleared employees to remind employees of their obligation to protect classified information and provide any updates to security requirements.

4.3. Debriefings

When a cleared employee no longer requires a security clearance or terminates employment with DSE, the employee will be debriefed by the FSO or the FSO's designated representative with oversight by the FSO.

4.4. Derivative Classification Training

DSE employees who have been authorized to make derivative classification decisions must complete initial derivative classification training and refresher training at least once every 2 years before being authorized to make derivative classification decisions. Documentation will be retained identifying the date of the most recent training and type of training derivative classifiers receive. Contact the FSO for guidance on how to access and complete the training.

5. Security Vulnerability Assessments/Self-Inspections

5.1. Defense Counterintelligence Security Agency

The Defense Counterintelligence Security Agency (DCSA) is the government cognizant security office (CSO) which provides oversight of contractors' procedures and practices for safeguarding classified defense information. Industrial Security Representatives of DSS may contact you in connection with the conduct of a security vulnerability assessment of the facility, an investigation of an unauthorized disclosure of classified information, or to provide advice and assistance to you and DSE on security related issues.

Our assigned DCSA field office is:
Defense Counterintelligence and Security Agency
Philadelphia Field Office
2 International Plaza, Suite 340
Philadelphia, PA 19113
610-537-1058

5.2. Security Vulnerability Assessments (SVA)

DSE will be assessed by DCSA on a cycle consistent with risk management principles. During this time, DCSA Industrial Security Representatives will review our security processes and procedures to ensure compliance with the 32 CFR part 117, and interview DSE employees to assess the effectiveness of the security program. Your cooperation with DCSA during the SVA is required.

5.3. Self-Inspections

DSE security staff will also perform a self-inspection, similar to the DCSA SVA. The purpose is to self-assess the security procedures to determine the effectiveness and identify any deficiencies/weaknesses. As part of this self-inspection, DSE employees will be interviewed. The results of the self-inspection will be briefed to employees during refresher briefings.

6. Individual Reporting Responsibilities

All DSE employees are to report any of the following information to the FSO. Our FSO (Don Selvy) can be reached at (410) 838-5073 or dselvy@dse-inc.net.

6.1. Espionage/Sabotage

Report any information concerning existing or threatened espionage, sabotage, or subversive activities. The FSO will forward a report to the FBI and DCSA.

6.2. Suspicious Contacts

Suspicious contacts are efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise cleared employees. Personnel should report all suspicious contacts to the FSO. The FSO forwards all reports to the respective government agency for review and action.

6.3. Adverse Information

Adverse information is any 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 or that his or her access to classified information may not be in the interest of national security. Cleared personnel report adverse information regarding himself, herself, or another cleared individual to the FSO. Reportable adverse information includes:

- Relationships with any known saboteur, spy, traitor, anarchist, or any espionage or secret agent of a foreign nation
- Serious mental instability or treatment at any mental institution
- Use of illegal substances or excessive use of alcohol or other prescription drugs
- Excessive debt, including garnishments on employee's wages
- Unexplained affluence/wealth
- Unexplained absence from work for periods of time that is unwarranted or peculiar
- Criminal convictions involving a gross misdemeanor, felony, or court martial
- Violations and deliberate disregard for established security regulations or procedures
- Unauthorized disclosure of classified information
- Members of, or individuals sympathetic to, an organization aiming to overthrow the U.S. Government by unconstitutional means.
- Involvement in the theft of, or any damage to, Government property

Note: Reporting adverse information does not necessarily mean the termination of a personnel clearance. Reports should not be based on rumor or innuendo.

6.4. Loss, Compromise, or Suspected Compromise of Classified Information

Cleared personnel must immediately report the loss, compromise, or suspected compromise of classified information.

6.5. Security Violations

Cleared personnel must report any failure to comply with a requirement of this SPP or of 32 CFR Part 117. See Section 7 regarding DSE's graduated scale of disciplinary actions.

6.6. Personal Changes

Cleared personnel report personal changes to include:

- Change in name
- Termination of employment
- Change in citizenship
- Access to classified information is no longer needed
- No longer wish to be processed for a personnel clearance or continue an existing clearance

6.7. Security Equipment Vulnerabilities

Personnel must report significant vulnerability in security equipment or hardware/software that could possibly lead to the loss or compromise of classified information.

7. Graduated Scale of Disciplinary Actions

DSE will use the following graduated scale of disciplinary actions as a guide in determining appropriate administrative actions to assign to security violations:

Security violations are recorded by the FSO through an Administrative Inquiry (AI) process. A copy of procedures for the AI process is maintained by the FSO and contains detailed guidance for collecting required data and making required reports within the mandatory timelines. Top Secret initial reports will be completed within 24 hours. Secret/Confidential initial reports will be completed within 72 hours. The FSO will conduct an investigation of the violation using the AI process.

In addition to disciplinary action that may be taken pursuant to other DSE policies, 32 CFR Part 117 requires a graduated scale of disciplinary actions in the event of employee violations or negligence.

(a) Minor violations will result in a review of proper security procedures with the individual. The Security Incident Report will be kept in the employee's security file in the Security Office.

(b) A second minor violation will result in the employee being required to participate in a complete review of 32 CFR Part 117 requirements. The Security Incident Report will be provided maintained in the employee personnel file and be provided to the management of the facility in which the violation occurred.

(c) Additional minor violations indicate a pattern of negligence and will result in an Adverse Information Report submitted to DCSA. The Security Incident Report and the Adverse Information Report will be provided to the management of the facility in which the classified work is being performed. A decision will be made by the FSO and the management of the facility where the violations occurred as to the appropriate corrective action to be taken which may be up to, and include, denying the individual access

to classified information. At the discretion of the President of DSE, the employee's employment at DSE may be terminated if it is determined failure to access classified information negatively impacts DSE's ability to accomplish tasking required on classified contracts.

(d) Major violations include the loss, compromise, and suspected compromise of classified information. Classified material that is out of the control of its custodian or that cannot be found shall be presumed to be lost until an investigation determines otherwise. If an investigation determines that classified material is lost, the employee will be denied access to classified information for a period of at least one year. The actual length of time for lack of access will be determined by the President of DSE and the management of the facility where the violation occurred. All major violations will be reported to the DCSA Field Office.

When individual responsibility for a security violation can be determined and one or more of the following factors are evident, an Individual Culpability Report will be sent to DCSA.

(a) Deliberate disregard of security requirements.

(b) Gross negligence in the handling of classified material.

(c) A pattern of negligence or carelessness.

8. Defense Hotline

The Department of Defense (DoD) provides a Defense Hotline as a confidential avenue for individuals to report allegations of wrongdoing pertaining to programs, personnel, and operations that fall under the purview of the Department of Defense, pursuant to the Inspector General Act of 1978. Anyone, including members of the public, DoD personnel and DoD contractor employees, may file a complaint with the DoD Hotline.

DEFENSE HOTLINE
THE PENTAGON
WASHINGTON, DC 20301-1900
TELEPHONE: 800-424-9098
http://www.dodig.mil/hotline

9. Marking Classified Information

9.1. Classification Levels

- ***TOP SECRET*** - Material that if compromised could cause "Exceptionally Grave" damage to national security and requires the highest degree of protection.
- ***SECRET*** - Material that if compromised could cause "Serious" damage to national security and requires a substantial degree of protection.
- ***CONFIDENTIAL*** - Material that if compromised could cause "Identifiable" damage to national security.

9.2. Original Classification

The determination to originally classify information may be made ONLY by a U.S. Government official who has been delegated the authority in writing. Information is classified pursuant to Executive Order 13526 and is designated and marked as Top Secret, Secret or Confidential. Contractors make derivative

classification decisions based on the guidance provided by the Contract Security Classification Specification (DD Form 254) and Security Classification Guidance applicable to each classified contract.

9.3. Derivative Classification

DSE 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. See Section 4.4 regarding required derivative classification training.

10. Classified Information

10.1. Classification Levels

- ***TOP SECRET*** - Material that if compromised could cause "Exceptionally Grave" damage to national security and requires the highest degree of protection.
- ***SECRET*** - Material that if compromised could cause "Serious" damage to national security and requires a substantial degree of protection.
- ***CONFIDENTIAL*** - Material that if compromised could cause "Identifiable" damage to national security.

10.2. Oral Discussions

DSE employees shall ensure that classified discussions will not take place over unsecure telephones, in public conveyances or places, or in any other manner that permits interception by unauthorized persons. If you need to have a classified discussion, contact the FSO to determine which areas have been designated for classified discussions.

10.3. End-of-Day Checks

To ensure that all storage containers are properly secured, the facility-unique procedures will be followed at the end of each business day. DSE does not store classified material or provide secured spaces for classified work on DSE property. Employees handling classified material in cleared customer spaces shall comply with local facility procedures including end-of-day responsibilities.

10.4. Perimeter Controls

DSE employees perform classified work in cleared customer spaces. There are no specific DSE perimeter controls. Consistent with our facility clearance, all visitors and employees are subject to possible inspection, which will occur at random intervals.

10.5. Receiving Classified Material

DSE is not authorized to receive classified material. Requests to hold or transport classified material shall be declined and referred to the owning activity.

10.6. Storage of Classified Information

DSE is not currently approved to store classified material. Employees shall not agree to transport, or store classified material outside cleared customer spaces.

10.7. Combinations

DSE does not maintain classified material storage facilities or safes requiring combination policies.

10.8. Transmission of Classified Information

DSE facilities are not authorized for transmission of classified information. All transmissions by DSE employees shall be in cleared customer spaces and comply with local facility requirements of the cleared customer facility.

10.9. Reproduction of Classified Material

Classified information may only be reproduced on equipment or copy machines that have been approved for classified reproduction at cleared customer sites. DSE does not maintain suitable copy machines for classified material. Reproduction or copying of classified material in DSE spaces or on DSE equipment is strictly prohibited.

10.10. Destruction of Classified Material

DSE does not store classified material but may perform classified work in customer spaces. Once classified material has served its purpose, it will be returned to the government customer or destroyed as soon as possible. Classified material will be destroyed in accordance with procedures in place at the cleared customer site. Contact the FSO for guidance.

10.11. Retention of Classified Materials

DSE is not authorized to store or retain classified materials.

11. Public Release/Disclosure

DSE is not permitted to disclose classified or unclassified information pertaining to a classified contract to the public without prior review and approval by the government customer. If you have a need to perform a presentation or create brochures, promotional sales literature, reports to stockholders, or similar materials, on subject matter related to a classified contract, even if unclassified, please see the FSO to determine if we must obtain approval from the customer.

Note: Classified information made public is not automatically considered unclassified. DSE personnel shall continue the classification until formally advised to the contrary.

12. Visit Procedures

12.1. Incoming Visits

DSE is not authorized to host classified meetings at DSE facilities. All incoming classified visits must be approved in advance of the visit by the FSO. The FSO will verify each visitor's security status prior to allowing classified access. The FSO is responsible for determining that the requesting contractor has been granted an appropriate facility clearance based upon an existing contractual relationship involving classified information of the same or higher classification category, or otherwise by verification through DISS.

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.

12.2. Outgoing Visits

All classified visits require advance notification to, and approval of, the place being visited. When it becomes necessary for employees of DSE to visit other cleared contractors or Government agencies and access to classified information is anticipated, employees must notify the FSO and provide the contractor or agency to be visited, the time and duration of visit, the reason for the visit, and the person to be contacted. Ample time must be allowed to permit the visit authorization request to be prepared, submitted via DISS to the contractor/agency, and processed by their visitor control.

13. Information System Security

DSE does not hold or maintain any classified information systems. Use of classified information at other cleared locations requires coordination with the local Information Systems Security Manager (ISSM). Contact the facility ISSM for review of System Security Plans (SSP) for all classified information systems. DSE does not maintain any SSPs.

NOTE: Classified information CANNOT be entered into any computer or other electronic device at DSE if it has not been formally approved/accredited for classified processing. If you have any question as to whether a system is approved, please contact the FSO.

14. Emergency Procedures

14.1. Emergency Plan

In emergency situations, it is important to safeguard all classified information as best as possible. However, the overriding consideration in any emergency is the safety of personnel. Do not risk your life or the lives of others to secure classified information. For example, in case of fire, you may need to immediately exit the facility with the classified materials in your possession. Seek out the FSO for further instructions once in a safe environment.

14.2. Emergency Contact Numbers

Name	Main #	Cell Phone #
Don Selvy (FSO)	(410) 838-5073	(410) 808-3511
KC Pake (Assistant FSO)	(410) 459-9601	(410) 459-9601

15. Definitions

The following definitions are common security related terms.

Access	The ability and opportunity to obtain knowledge of 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 be in the interest of national security.
Authorized Person	A person who has a need-to-know for the classified information involved and has been granted a personnel clearance at the required level.
Classified Contract	Any contract that requires, or will require, access to classified information by the contractor or its employees in the performance of the contract.
Classified Information	Official Government information which has been determined to require protection against unauthorized disclosure in the interest of national security.
Cleared Employees	All DSE employees granted a personnel clearance or who are in process for a personnel clearance.
Closed Area	An area that meets the requirements outlined in the NISPOM for safeguarding classified information that, because of its size, nature, and operational necessity, cannot be adequately protected by the normal safeguards, or stored during nonworking hours in approved containers.
Communication Security (COMSEC)	COMSEC 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.
Compromise	An unauthorized disclosure of classified information.
CONFIDENTIAL	Classified information or material that requires protection whereby unauthorized disclosure could reasonably be expected to cause damage to our national security.
Facility (Security) 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, chartered, or incorporated under the laws of any country other than the United States or its territories, and any person who is not a citizen or national of the United States.
Foreign National	Any person who is not a citizen or national of the United States.
Need-to-Know (NTK)	A determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information to perform tasks or services to fulfill a classified contract or program.
Personnel Security Clearance (PCL)	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.
Public Disclosure	The passing of information and/or material pertaining to a classified contract to the public or any member of the public by any means of communication.
SECRET	Classified information or material that requires a substantial degree of protection, the unauthorized disclosure of which could reasonably be expected to cause serious damage to our national security.
Security Violation	Failure to comply with policy and procedures established by the NISPOM that could reasonably result in the loss or compromise of classified information.
Standard Practice Procedures (SPP)	A document prepared by contractors outlining the applicable requirements of the NISPOM for the contractor's operations and involvement with classified information at the contractor's facility.
Subcontractor	A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor.
TOP SECRET	Classified information or material that requires the highest degree of protection, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to our national security.

Unauthorized Person	A person not authorized to have access to specific classified information in accordance with the requirements of the NISPOM.

16. Abbreviations & Acronyms

AFSO	Assistant Facility Security Officer
AIS	Automated Information System
C	Confidential
CAGE	Commercial and Government Entity
COMSEC	Communication Security
CSA	Cognizant Security Agency
CSO	Cognizant Security Office
DoD	Department of Defense
DoD CAF	Department of Defense Central Adjudication Facility
DOE	Department of Energy
DTIC	Defense Technical Information Center
e-QIP	Electronic Questionnaires for Investigation Processing
FBI	Federal Bureau of Investigation
FCL	Facility (Security) Clearance
FSO	Facility Security Officer
GCA	Government Contracting Activity
GSA	General Services Administration
ISFD	Industrial Security Facilities Database
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ITAR	International Traffic in Arms
KMP	Key Management Personnel
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NTK	Need-To-Know
OPM	Office of Personnel Management
PCL	Personnel Security Clearance
POC	Point of Contact
PR	Periodic Reinvestigation
PSMO-I	Personnel Security Management Office for Industry
S	Secret
SCG	Security Classification Guide
SPP	Standard Practice Procedures
TS	Top Secret
U	Unclassified
US	United States

17. References

[1] 32 Code of Federal Regulation (CFR) Part 117, NISPOM (National Industrial Security Program Operating Manual.