

STANDARD PRACTICES AND PROCEDURES (SPP)

Research and Engineering Development, LLC

48015-1 Pine Hill Run Road

Lexington Park, MD 20653

Foreword

Research and Engineering Development, LLC (RED-INC) 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.

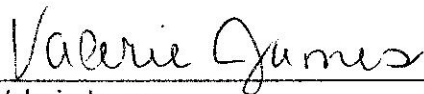
Some of our programs and activities are vital parts of the defense and security systems of the United States. All of us – both management and individual employees – are responsible for properly safeguarding the classified information entrusted to our care.

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 company 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.



David Aldrich
Chief Executive Officer



Valerie James
Facility Security Officer

Table of Contents

1. Introduction	3
2. Facility Information	3
2.1. Facility Clearance	3
2.2. Facility Security Officer	3
2.3. Storage Capability	3
3. Personnel Security Clearances.....	3
3.1. Clearance Procedures	3
3.2. Reinvestigations.....	4
3.3. Consultants	4
4. Security Education	5
4.1. Initial Security Briefings	5
4.2. Annual Security Briefings.....	5
4.3. Debriefings.....	5
5. Security Vulnerability Assessments/Self-Inspections	5
5.1. Defense Security Service.....	5
5.2. Security Vulnerability Assessments (SVA)	5
5.3. Self-Inspections.....	6
6. Individual Reporting Responsibilities	6
6.1. Espionage/Sabotage	6
6.2. Suspicious Contacts.....	6
6.3. Adverse Information	6
6.4. Loss, Compromise, or Suspected Compromise of Classified Information.....	7
6.5. Security Violations	7
6.6. Personal Changes.....	7
7. Graduated Scale of Disciplinary Actions	7
8. Defense Hotline	7
9. Classified Information.....	8
9.1. Classification Levels	8
9.2. Oral Discussions	9
9.3. Transmission of Classified Information.....	9

9.4. Retention of Classified Materials..... 10

10. Public Release/Disclosure 10

11. Visit Procedures..... 11

 11.1. Incoming Visits 11

 11.2. Outgoing Visits 11

12. Emergency Procedures..... 11

 12.1. Emergency Plan..... 11

 12.2. Emergency Contact Numbers 11

13. Definitions 11

14. Abbreviations & Acronyms..... 13

15. References..... 13

1. Introduction

This Standard Practices and Procedures (SPP) describes RED-INC's 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], 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. RED-INC has a Top Secret facility clearance. The FCL is valid for access to classified information at the Top Secret or lower classification level.

2.2. Facility Security Officer

Having a facility clearance RED-INC 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. Valerie James is the FSO for RED-INC and can be reached at valerie.james@red-inc.us or 301-737-4361 ext. 23.

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. RED-INC contracts authorize access to classified information only at another contractor's facility or a government activity. Employees accessing classified information at these sites are required to follow the security procedures and requirements of the facility or installation.

3. Personnel Security Clearances

3.1. Continuous Evaluation Program/Employee Responsibility

Employees who hold a security clearance are expected to maintain the clearance in accordance with the government's Continuous Evaluation Program (CEP). Once an employee has been granted access to classified information through the initial favorable eligibility determination, the employee falls under the CEP as long as access to classified information or material is contractually required. By definition, CEP involves the uninterrupted assessment of an individual in order to retain a security clearance. CEP includes reinvestigation at given intervals based on the level of access to classified information.

The Facility Security Officer (FSO) is responsible for initiating the background investigation at the appropriate interval and will communicate with the employee, providing guidance and direction to complete the process. Currently, investigations may be initiated 90 days prior to the closing date of the previous investigation in the investigation year. An investigation is considered to be "out of scope" (i.e., overdue) on the 91st day. If after 90 days the investigation has not been submitted to the Office of

Personnel Management (OPM) for review / approval due to inattention on the part of the employee (as determined by the FSO) the employee will receive a written warning that failure to complete the process within 10 days will result in access to classified information being suspended until the application has been submitted to OPM. Noncompliance may result in termination at the discretion of the CEO.

Not being in compliance with requirements and allowing a background investigation to go out of scope puts an employee at risk of being issued a Loss of Jurisdiction which effectively ends the employee's access to classified information. If tasking requires a clearance and the employee is issued a Loss of Jurisdiction due to noncompliance it will effectively end the employee's work on the contract.

3.2. Clearance Procedures

RED-INC 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.

RED-INC will utilize the Joint Personnel Adjudication System (JPAS) 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 a copy of NISPOM paragraph 2-202. 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 RED-INC initiates the clearance process for employees, the government will make the determination of whether or not an individual is eligible to access classified information and grant the personnel clearance.

3.3. 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.

3.4. Consultants

For security administration purposes, consultants are treated as employees of RED-INC 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 RED-INC sponsors a consultant for a PCL, the consultant must be compensated directly by RED-INC; otherwise, the company receiving compensation must obtain a Facility Security Clearance (FCL) and serve as a subcontractor to RED-INC.

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 in order 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 RED-INC, the employee will be debriefed by the FSO.

5. Security Vulnerability Assessments/Self-Inspections

5.1. Defense Security Service

The Defense Security Service (DSS) 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 RED-INC on security related issues.

Our assigned DSS field office is:

Defense Security Service (IOFCS2)
2331 Mill Road, 4th Floor
Alexandria, VA 22314
Phone: 703-617-2331

5.2. Security Vulnerability Assessments (SVA)

RED-INC will be assessed by the DSS on an annual cycle. During this time, DSS Industrial Security Representatives will review our security processes and procedures to ensure compliance with the NISPOM, and interview RED-INC employees to assess the effectiveness of the security program. Your cooperation with DSS during the SVA is required.

5.3. Self-Inspections

RED-INC security staff will also perform a self-inspection, similar to the DSS 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, RED-INC employees will be interviewed. The results of the self-inspection will be provided to management and the CSO and briefed to employees during refresher briefings.

6. Individual Reporting Responsibilities

All RED-INC employees are to report any of the following information to the FSO. Our FSO, Valerie James, can be reached at valerie.james@red-inc.us or 301-737-4361 ext. 23.

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 DSS.

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 to the government sponsor as well as the RED-INC Facility Security Officer.

6.5. Security Violations

Cleared personnel must report any failure to comply with a requirement of this SPP or of the NISPOM. See Section 7 regarding RED-INC’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

7. Graduated Scale of Disciplinary Actions

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

Level of Violation	Examples (not all inclusive)	Minimum Disciplinary/Corrective Action
Level 1 – Verbal Warning	<ul style="list-style-type: none"> • Password sharing or allowing access using your password • First offense of unintentional infraction 	Verbal warning or discussion from Facility Security Officer (FSO)/Director and notification to Chief Executive Officer (CEO). A memo will be placed in the employee security file documenting that a verbal warning was issued.
Level 2 – Written Warning	<ul style="list-style-type: none"> • Unauthorized use of company or government IT systems • Failure to timely comply with company security procedures or initiatives • Repeated behavior following a verbal warning 	Written warning coordinated with FSO, Director, and CEO. May include attendance at required training or security refresher. A copy of the warning letter will be kept in the employee HR and security folders.
Level 3 – Suspension Without Pay	<ul style="list-style-type: none"> • Violation or infraction for personal gain • Unintentional violation related to safeguarding of sensitive or classified information 	Written notification of suspension coordinated with HR, FSO and CEO. Meeting with employee to include FSO, CEO, and Director. May result in termination of computer access or

		restricted area access. May include attendance at required training or security refresher. Suspensions may vary in length, according to the severity of the offense or deficiency. A copy of the suspension letter will be filed in the employee HR and security folders.
Level 4 - Termination	<ul style="list-style-type: none"> • Repeated violations of Levels 1-3 or where evidence clearly establishes malicious intent • Violation or infraction with the intent to harm an individual, the company, or the nation • No evidence of substantial improvement in conduct on the part of the employee following suspension • First time incident extremely serious in nature 	Written notification of termination to be signed by cognizant managing official. The employee will be escorted from the property by the company FSO.

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 DOD, 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. 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. Oral Discussions

RED-INC employees shall ensure that classified discussions do not take place in our facility. Since we are not authorized to store classified information our facility is not equipped with secure telephones or spaces and is considered a public conveyance that could permit interception by unauthorized persons. If you need to have a classified discussion, contact the sponsor at the facility where you work to determine which areas have been designated for classified discussions.

9.3. Transmission of Classified Information

When it becomes necessary for classified material to be sent to another location, the following procedures will apply:

The installation cognizant classified information owner shall:

1. Approve transmission of classified material
2. Prepare 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 1) be addressed (both sender and recipient addresses), 2) be marked on all sides with the appropriate classification level, and 3) contain the receipt
 - The outer container or wrapping will reflect the classified mailing address and return address only

9.3.1. Courier Procedures

RED-INC employees who hand-carry classified material from NAS Patuxent River must satisfy all the following requirements for couriers:

- Cleared to the appropriate level required for the most restrictive classification of the material to be hand-carried
- Designated in writing on company letterhead to perform courier duties by the FSO
- Briefed on courier responsibilities to safeguard classified information when designated by the FSO
- Possess an identification card or badge which contains the employee's name and photograph

9.3.2. Courier Requirements

Employees designated as a courier for the transmission of Department of Defense classified material must 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 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 classified material essential for the purpose of a visit is being carried.
4. The material must be prepared and packaged in accordance with the installation's policies and procedures. 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 installation's security office. Custody of classified material will not be accepted nor will release of classified material be allowed without the exchange of receipts.

5. While traveling, couriers are required to proceed directly to the facility designated to receive the material. Couriers are personally responsible for the protection and proper delivery of the classified material entrusted to their care. Couriers must conduct themselves in such a manner that the security of the classified material in their care will not result in prejudice or be compromised through carelessness or lack of vigilance. The fact that classified material is being transported 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 which may impair the judgment or physical capabilities of an individual may not be used while having custody of classified material.
7. Classified material must be continuously in the possession of the courier 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 constant surveillance; therefore, couriers may not sleep while such material is in their possession.
8. During any stopover, the classified material will remain under the constant surveillance of the courier unless arrangements have been made in advance of 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 the government sponsor and the RED-INC Security Officer. If a problem arises and assistance is not available, contact the nearest U.S. Government activity or cleared contractor facility for assistance.

9.4. Retention of Classified Materials

Classified materials may be retained for two years after the conclusion of the classified contract under which they were received. Before two years has passed, retention authority must be requested in writing to the government activity. Contact the FSO for guidance.

10. Public Release/Disclosure

RED-INC 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 government sponsor or the company FSO to determine if we must obtain approval from the customer.

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

11. Visit Procedures

11.1. Incoming Visits

RED-INC is not authorized to store classified information; therefore, classified visits are not authorized at our facility.

11.2. Outgoing Visits

All classified visits require advance notification to, and approval of, the place being visited. When it becomes necessary for employees of RED-INC to visit other cleared contractors or Government agencies and access to classified information is anticipated, employees must notify the FSO and provide the Security Management Office (SMO) of the contractor or agency to be visited, the date(s) and duration of visit, the reason for the visit, and the name and phone number of the person with whom you will be visiting. Ample time must be allowed to permit the visit authorization request to be prepared, submitted via JPAS to the contractor/agency, and processed by their visitor control.

12. Emergency Procedures

12.1. Emergency Plan

In emergency situations, it is important to safeguard all classified information as best as possible. However, the overriding consideration in any emergency situation is the safety of personnel. Do not risk your life or the lives of others in order 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 cognizant classified information owner and contact the company Facility Security Officer for further instructions once in a safe environment.

12.2. Emergency Contact Numbers

Name	Main #	Cell Phone #
Valerie James	301-737-4361 ext 23	240-577-1062
John Sison	301-737-4361 ext 45	240-298-4846

13. 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.

<i>Cleared Employees</i>	All RED-INC employees granted a personnel clearance or who are in process for a personnel clearance.
<i>Closed Area</i>	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.
<i>Communication Security (COMSEC)</i>	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.
<i>Compromise</i>	An unauthorized disclosure of classified information.
<i>CONFIDENTIAL</i>	Classified information or material that requires protection whereby unauthorized disclosure could reasonably be expected to cause damage to our national security.
<i>Facility Security Clearance (FCL)</i>	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).
<i>Foreign Interest</i>	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.
<i>Foreign National</i>	Any person who is not a citizen or national of the United States.
<i>Need-to-Know (NTK)</i>	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 in order to perform tasks or services to fulfill a classified contract or program.
<i>Personnel Security Clearance (PCL)</i>	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.
<i>Public Disclosure</i>	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.
<i>SECRET</i>	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.
<i>Security Violation</i>	Failure to comply with policy and procedures established by the NISPOM that could reasonably result in the loss or compromise of classified information.
<i>Standard Practice Procedures (SPP)</i>	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.
<i>Subcontractor</i>	A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor.
<i>TOP SECRET</i>	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.
<i>Unauthorized Person</i>	A person not authorized to have access to specific classified information in accordance with the requirements of the NISPOM.

14. 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
DSS	Defense Security Service
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
JPAS	Joint Personnel Adjudication System
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

15. References

- [1] [National Industrial Security Program Operating Manual \(NISPOM\)](#), DOD 5220.22-M.