STANDARD PRACTICES AND PROCEDURES (SPP)

360 Patriot Enterprises LLC.

1 February 2022

Forward

360 Patriot Enterprises LLC, hereafter referred to as Patriot Enterprises, 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 32 CFR NISPOM RULE. 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 32 CFR NISPOM RULE 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.

Michel J. Owen
CEO Patriot Enterprises
Senior Management Official

Cynthia A. Dillard
Facility Security Officer

PATRIOT ENTERPRISES

Table of Contents

1. Introduction

This Standard Practices and Procedures (SPP) describes Patriot Enterprises 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 (32 CFR NISPOM RULE)[1], which takes precedence in instances of apparent conflict.

2. Facility Information 117.9

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. Patriot Enterprises 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 Patriot Enterprises has agreed 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. The FSO for Patriot Enterprises and can be reached at Security@PatriotEnterprisesLLC.com or 866-694-9516.

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. Patriot Enterprises has **NOT** been approved to store classified material.

3. Personnel Security Clearances 117.10

3.1. Clearance Procedures

Patriot Enterprises 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.

Patriot Enterprises 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 the information from 32 CFR NISPOM RULE 117.10 (d)(1)(2). 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.

Commitment for Employment – REF 117.10 (f)(1)(i)(ii)(f)(2)(3)

While Patriot Enterprises 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. Our FSO is responsible for reviewing all access records to ensure employees are submitted for PRs as required.

3.3. Consultants – 117.10 (m)

For security administration purposes, consultants are treated as employees of Patriot Enterprises and must comply with this SPP and the 32 CFR NISPOM RULE. Consultants will, however, be required to execute a Consultant Agreement which outlines any security responsibilities specific to the consultant.

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

4. Security Education 117.12

4.1. Initial Security Briefings – (117.12) (e)

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 briefings include the following:

1. Threat Awareness Briefing, including Insider Threat awareness
2. Counterintelligence CI Awareness
3. Overview of Security Classification System
4. Employee reporting obligations and requirements, including insider threat
5. Cybersecurity training for all authorized information systems users
6. Security procedures and duties applicable to the employee's position requirements (e.g. marking and safeguarding of classified information)
7. Criminal, civil, or administrative consequences that may result from the unauthorized disclosure of classified information, even though the individual has not yet signed an NDA.
8. Insider Threat Training
9. CUI training (While outside the requirements of the NISPOM, when a classified contract includes provisions for CUI training, contractors will comply with those contract requirements)
10. Overview of the SPP

4.2. Annual Security Briefings – 117.12 (k)

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 117.12 (L)

When a cleared employee no longer requires a security clearance or terminates employment with Patriot Enterprises, the employee will be debriefed by the FSO and out-processed from DISS.

4.4. Derivative Classification Training – 117.12 (h) (1) & (2)

Patriot Enterprises 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 Reviews/Self-Inspections - 117.7

5.1. Defense Counterintelligence and Security Agency

The Defense Counterintelligence and 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 DCSA 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 Patriot Enterprises on security related issues. Our assigned DCSA field office is:

National Access Elsewhere Security Oversight Center (NAESOC)
7556 Teague Road, Suite 500
Hanover, MD 21076

5.2. Security Reviews (SR)

Patriot Enterprises will be assessed by the DCSA on a 12-18 month cycle. During this time, DCSA Industrial Security Representatives (ISR) will review our security processes and procedures to ensure compliance with the 32 CFR NISPOM RULE, and interview Patriot Enterprises employees to assess the effectiveness of the security program. Your cooperation with DCSA during the SR is required.

5.3. Self-Inspections – 117.7 (g)(2)

Patriot Enterprises security staff will also perform a self-inspection, similar to the DCSA ISR. The purpose is to self-assess the security procedures to determine the effectiveness and identify any deficiencies/weaknesses. As part of this self-inspection, Patriot Enterprises employees will be interviewed. The results of the annual self-inspections are available to cleared employees upon request.

6. Individual Reporting Responsibilities -- SEAD 3 – 117.8

All Patriot Enterprises employees are to report any of the following information to the FSO. Our FSO can be reached at Security@PatriotEnterprisesLLC.com or via phone at 866-694-9516. Reporting

requirements can be found at https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf

The following is a list, though not all conclusive, of reportable incidents and actions:

6.1. Unofficial Foreign Travel 117-18 (a)

1. Covered individuals shall submit an itinerary for unofficial foreign travel to their government lead and, except as noted in the subparagraphs below, must receive approval from the government prior to the foreign travel. Covered individuals must also notify the Patriot Enterprises' FSO who will in turn provide the requisite security briefings in accordance with the company's security program. Unanticipated border crossings into any foreign country not included in the traveler's approved itinerary, regardless of duration, are discouraged. All deviations from approved travel itineraries shall be reported to both the government and the company within five business days of return.
2. Travel to Puerto Rico, Guam, or other U.S. possessions and territories is not considered foreign travel and need not be reported.
3. Unplanned day trips to Canada or Mexico shall be reported upon return. Reporting shall be within five business days.
4. All Patriot covered individuals shall, prior to unofficial foreign travel, receive a defensive security and counterintelligence briefing. Full reporting and debriefing shall be scheduled prior to travel and accomplished upon return.
5. While emergency circumstances may preclude full compliance with pre-travel reporting requirements, the covered individual, at a minimum, shall verbally advise their supervisor/management chain of the emergency foreign travel with all pertinent specifics and, preferably, a security representative, prior to departure. In any event, full reporting shall be accomplished within five business days of return.
6. Consistent with national security, heads of agencies or designees may identify, for covered individuals under their purview, conditions under which prior reporting and approval of unofficial travel is not required, such as, agencies with an overseas presence that may require less specific reporting as opposed to every instance, e.g. travelled to x country y times last month, travel weekly/monthly to x country, travel to x country y times per year, etc.
7. Heads of agencies or designees may disapprove an unofficial foreign travel request when it is determined that such travel presents an unacceptable risk and the physical safety and security of covered individuals or classified information cannot be reasonably ensured. Failure to comply with such disapproval may result in administrative action that includes, but is not limited to, revocation of national security eligibility.

6.2. Foreign Contacts 117-18 (a)

1. Unofficial and limited contacts with a known or suspected foreign intelligence entity must be reported.
2. Continuing association with known foreign nationals that involve bonds of affection, personal obligation, or intimate contact; or any contact with a foreign national that involves the exchange of personal information must be reported. This reporting requirement is based on the nature of the relationship regardless of how or where the foreign national contact was made or how the relationship is maintained (i.e., via personal contact, telephonic, postal system, Internet, etc.).

Following initial reporting, updates regarding continuing unofficial association with known foreign nationals shall occur only if there is a significant change in the nature of the contact.

3. The reporting of limited or casual public contact with foreign nationals is not required absent any other reporting requirement in this directive.
4. Heads of agencies or designees may provide specific guidance and examples of updated reporting situations.

6.3. Reportable Actions on Yourself or by Others 117-18 (c)(1)(i)(ii)

To ensure the protection of classified information or other information specifically prohibited by law from disclosure, covered individuals shall alert their FSO to the following reportable activities of themselves or other covered individuals that may be of potential security or counterintelligence (CI) concern:

1. An unwillingness to comply with rules and regulations or to cooperate with security requirements.
2. Unexplained affluence (in excess of $10,000) or excessive indebtedness (to include bankruptcy or any past due indebtedness more than 120 days).
3. Any arrest by a local, state, or Federal officer
4. Alcohol abuse.
5. Illegal use or misuse of drugs or drug activity – to include marijuana and CBD use. While these products may be legal in a state, they are still illegal under Federal Law and are therefore reportable.
6. Ownership of stock which primary business is the growth, processing and/or sale of marijuana products.
7. Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified information or other information specifically prohibited by law from disclosure.
8. Criminal conduct.
9. Any activity that raises doubts as to whether another covered individual's continued national security eligibility is clearly consistent with the interests of national security.
10. Misuse of U.S. Government property or information systems.
11. Ownership if Crypto Currency if the crypto currency is foreign state-backed, hosted, or managed cryptocurrency and ownership of cryptocurrency wallets hosted by foreign exchanges. No reporting is required if the covered individual holds crypto currency, but is NOT aware that any such holdings are backed, hosted, or managed by a foreign state, or that a cryptocurrency wallet is hosted by a foreign exchange. No reporting is required if the covered individuals' investments in cryptocurrency are held in a widely diversified fund (e.g. index funds), unless the investment instrument is entirely composed of holdings in cryptocurrency that is backed, hosted, or managed by a foreign state.
12. Contact with the media.

6.4. Espionage/Sabotage – 117.18 (a) (2)(iii)

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

6.5. Suspicious Contacts – 117.18 (c)(2)

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.

6.6. Adverse Information - 117-18 (c)(1)(i)(ii)

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:

1. Relationships with any known saboteur, spy, traitor, anarchist, or any espionage or secret agent of a foreign nation
2. Serious mental instability or treatment at any mental institution
3. Use of illegal substances or excessive use of alcohol or other prescription drugs
4. Excessive debt (Bankruptcy or past due indebtedness of more than 120 days), including garnishments on employee's wages
5. Unexplained affluence/wealth (in excess of $10,000)
6. Unexplained absence from work for periods of time that is unwarranted or peculiar
7. Criminal convictions involving a gross misdemeanor, felony, or court martial
8. Violations and deliberate disregard for established security regulations or procedures
9. Unauthorized disclosure of classified information
10. Members of, or individuals sympathetic to, an organization aiming to overthrow the U.S. Government by unconstitutional means.
11. 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.

6.7. Loss, Compromise, or Suspected Compromise of Classified Information – 117.8 (d)

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

6.8. Security Violations 117.8 (d)

Cleared personnel must report any failure to comply with a requirement of this SPP or of the 32 CFR NISPOM RULE. See Section 7 regarding Patriot Enterprises' graduated scale of disciplinary actions.

6.9. Personal Changes 117-18 (c)(3-6)

Cleared personnel must report personal changes, and send the supporting documentation, to the FSO. These changes include:

1. Change in name

2. Termination of employment
3. Change in citizenship
4. Access to classified information is no longer needed
5. No longer wish to be processed for a personnel clearance or continue an existing clearance

6.10. Security Equipment Vulnerabilities 117-18 (a)

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

6.11. Reporting Procedures.

Company personnel must report any reportable incident directly to Patriot Enterprises' FSO. Reports may be made via email, phone call or face to face. The FSO can be reached at 866-694-9516 or Security@PatriotEnterprisesLLC.com .

6.12. Processing Reports.

Unclassified reports as well as private, personnel reports will be stored in a separate electronic storage file with access limited to the FSO and Assistant FSO.

As Patriot Enterprises does not safeguard classified material, any incidents regarding loss or compromise of classified material will be coordinated at and with the cleared contracting facility or government agency where the incident occurred.

All sensitive, unclassified, reports will be reviewed and researched by the FSO to insure they are credible, and once deemed credible, they will be reported to DCSA and/or the FBI as required by the FSO.

6.13. Notification Process.

Employees at Patriot Enterprises will report any credible concerns regarding cleared employees directly to the FSO, preferably via phone or an in-person meeting. It is the responsibility of the FSO to investigate these reports for credibility and if found credible to report them as required to DCSA or the FBI. Personnel incident reports will be submitted via DISS. Loss of classified material will be reported, withholding any classified information, directly to DCSA as well as the government agency and if necessary, the cleared contractor involved in the loss. Threats of espionage or suspicious contacts will be submitted to both DCSA and the FBI.

7. Graduated Scale of Disciplinary Actions – 117.8 (e)(2)

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

If an employee is involved in one or more security violations, the following scale of disciplinary actions will be followed:

1. First Violation:

    a. The employee will be counseled by the Facility Security Officer
    b. A note describing the event will be placed in the employee's security folder
    c. The employee's supervisor will be informed about the violation.

d. If the violation included loss or compromise of classified material than a report must be filled with DSS.

2. Second Violation within a 12-month period:

a. The employee will be counseled by the Facility Security Officer
b. A formal notice of the incident will be put in the employee's security folder
c. A report will be filed with the Defense Counter-Intelligence Security Agency (DCSA)
d. The employee's direct supervisor and division manager will be informed about the violation.
e. Formal disciplinary actions up to suspension without pay may be assessed.

3. Third Violation within a 12-month period:

a. A formal notice of the incident will be put in the employee's security folder.
b. A report will be filed with the Defense Counter-Intelligence Security Agency (DCSA)
c. The employee's management team, including the company president or CEO will be advised of the violation.
d. Formal disciplinary actions up to employment termination may be assessed.

8. Defense Hotline – 117.7 (i)

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. Markings on Information – 117.13

9.1. Levels of Markings

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

3. ***CONFIDENTIAL*** - Material that if compromised could cause "Identifiable" damage to national security.

4. ***CUI*** – Controlled Unclassified Information – Sensitive Material that requires additional protections.

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

Patriot Enterprises 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. Safeguarding Classified Information – 117.15

10.1. Classification Levels

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

10.2. Oral Discussions

Patriot Enterprises 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. At this time Patriot Enterprises is not approved for classified meetings. If you need to have a classified discussion, contact the FSO to determine which areas have been designated for classified discussions.

11. Public Release/Disclosure – 117.15

Patriot Enterprises 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. Patriot Enterprises personnel shall continue the classification until formally advised to the contrary.

12. Visit Procedures – 117.16

12.1. Incoming Visits

At this time Patriot Enterprises is not approved for classified meetings. If it is determined that you need to hold a classified meeting it must be hosted at either the government's cleared work area or at a cleared government contracting company, approved for classified meetings, with whom Patriot Enterprises shares a contractual obligation to discuss the classified material.

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 Patriot Enterprises 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 – (Only for Approved Classified Systems)

NOTE: Classified information CANNOT be entered into any computer or other electronic device at Patriot Enterprises. Patriot Enterprises has not been formally approved/accredited for classified processing.

14. Emergency Procedures – 117.15 (a)(3)(iv)

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. Contact Information

Name	Phone #	Email
FSO, ITPSO, AFSO	866-694-9516	Security@PatriotEnterprisesLLC.com
DCSA, NAESOC	888-282-7682	DCSA.NAESOC.generalmailbox@mail.mil

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 Patriot Enterprises 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 32 CFR NISPOM RULE 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 32 CFR NISPOM RULE 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 32 CFR NISPOM RULE 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 32 CFR NISPOM RULE.

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
CUI	Controlled Unclassified Information
DoD	Department of Defense
DoD CAF	Department of Defense Central Adjudication Facility
DCSA	Defense Counterintelligence and Security Agency
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
ITPSO	Insider Threat Program Security Officer
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

17. References

[1] National Industrial Security Program Operating Manual (32 CFR 117 NISPOM Rule),

[2] DoDM 5220.32 Vol 1

[3] DoDM 5200.01 Vol 3

[4] 32 CFR Parts 2001 and 2003 Classified National Security Information; Final Rule

[5] Contractors Graduated Scale of Discipline.

[6] Contractor can provide other References as Needed.