SECURITY STANDARD PRACTICES AND PROCEDURES (SPP)

TACTICAL ELEMENT, INCORPORATED
11242 CR 229
Oxford, Florida 34484

Forward

Tactical Element, Incorporated (hereinafter **Tactical Element**) 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 – both management and individual employees – are responsible for properly safeguarding the classified information entrusted to our care.

Tactical Element's Standard Practice Procedures (SPP) conforms to the security requirements set forth in the government manual – the National Industrial Security Program Operating Manual or 32 CFR 117 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 117 NISPOM RULE is available for review by contacting the Facility Security Officer.

Tactical Element 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.

Amy L. Heath
President / CEO
Assistant Facility Security Officer

Donald C. Heath, Jr.
Vice President / COO
Facility Security Officer

Table of Contents

1. Introduction

This Standard Practices and Procedures (SPP) describes Tactical Element'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 (32 CFR 117 NISPOM RULE), which takes precedence in instances of apparent conflict. The governmental agency overseeing the 32 CFR 117 NISPOM Rule is Defense Counterintelligence and Security Agency (DCSA) which ultimately falls under the Department of Defense.

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. Tactical Element 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 Tactical Element 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 the required training and is responsible for supervising and directing security measures necessary for implementing the NISPOM and related Federal requirements for classified information. **Donald C. Heath, Jr.** is the FSO for Tactical Element and can be reached at 352-459-4186 or dch5657@tacticalelement.com. **Amy L. Heath** is the Assistant FSO (AFSO) for Tactical Element and can be reached at 352-459-4186 or alh1026@tacticalelement.com.

2.3. Storage Capability

The facility clearance level is separate from the storage capability level. Contractors must receive separate approval prior to storing any classified information. Tactical Element has been approved to store classified material up to the SECRET level. Section 9 and 10 discuss the procedures for appropriate handling, storage, and control of classified materials within our facility.

2.4. Facility Security Officer Reporting Requirements

Having a facility clearance Tactical Element has agreed and is now required to report various things impacting or associated with us. Some of the reporting conditions are:

- Changes in ownership, address, previously approved safeguarding conditions impacting classified storage.
- Changes in key management personnel like the FSO, Insider Threat Program Senior Official (ITPSO), officers and directors
- Changes impacting answers to the SF328 form – Certificate Pertaining to Foreign Interest
- Any cyber intrusions to our information systems, may this be for classified or unclassified

3. Personnel Security Clearances 117.10

3.1. Clearance Procedures

Tactical Element 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.

Tactical Element will utilize the Defense Information Security System (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 a copy of 32 CFR 117 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 1974.

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

While Tactical Element 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.

3.2. 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. The time when a PR is required and the length between PRs can change based on guidance from DCSA and the Vetting Risk Operations (VRO); VRO is a department within DCSA. Tactical Element 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 who are accessing classified information are treated as employees of Tactical Element and must comply with this SPP and the 32 CFR 117 NISPOM RULE. Consultants will, however, be required to execute a Consultant Agreement which outlines any security responsibilities specific to the consultant.

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

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 briefing will include the following:

- Threat Awareness Briefing, including Insider Threat Awareness
- Counterintelligence CI Awareness
- Overview of Security Classification System
- Employee reporting obligations and requirements, including insider threat
- Cybersecurity training for all authorized information systems users
- Security procedures and duties applicable to the employee's position requirements (e.g. marking and safeguarding of classified information)
- 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.
- Insider Threat Training
- 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.
- 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. The 32 CFR 117 NISPOM RULE defines annual for the time between security briefings as every 12 months.

4.3. Debriefings 117.12 (L)

When a cleared employee no longer requires a security clearance or terminates employment with Tactical Element, the employee will be debriefed by the FSO.

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

Tactical Element 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/Insider Threat Program - 117.7/117.12

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 (ISR) of DCSA may contact you in connection with conducting a security review of the facility, an investigation of an unauthorized disclosure of classified information, or to provide advice and assistance to you and Tactical Element on security related issues.

Our assigned DCSA field office is:

Defense Counterintelligence and Security Agency (DCSA)
7341 Office Park Place, Suite 203
Melbourne, FL 32940

5.2. Security Reviews (SR)

Tactical Element will be assessed by DCSA on an interval DCSA determines as needed based on our security posture and ongoing situations. During this time, DCSA Industrial Security Representatives (ISR) will review our security processes and procedures to ensure compliance with the 32 CFR 117 NISPOM RULE, and interview Tactical Element employees (cleared/uncleared) 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)

Tactical Element security staff will also perform a self-inspection, like the DCSA SR. The purpose is to self-assess the security procedures to determine the effectiveness and identify any deficiencies/weaknesses. As part of this self-inspection, Tactical Element employees will be interviewed. The results of the self-inspection will be briefed to employees during refresher briefings normally. A memo will be completed for the senior management official addressing the following items as they apply to our facility:

- Self-inspection has been conducted on the security and insider threat program - date.
- Sample of derivatively generated holdings reviewed - if applies.
- Senior management has been briefed on the results.
- Appropriate corrective action has been taken as needed for vulnerabilities noted.
- Facility profile in NISS which includes contracts has been verified.
- Comment on validation of excluded parent information - if applies.
- Recommendations; and
- Management fully supports the security program at the cleared facility.

The memo is then uploaded into National Industrial Security System (NISS) by our FSO under the Self-Inspection tab; self-inspections per 32 CFR 117 NISPOM RULE must be conducted at least annually (every 12 months) unless directed otherwise by DCSA and/or our assigned ISR.

5.4. Insider Threat Program – 117.12 (g)

Tactical Element has developed a required Insider Threat Program with the main emphasis of recognizing a possible insider threat and preventing an insider threat from occurring. Part of prevention is developing a program through awareness, education, and training. All of us play a critical role in preventing insider threat incidents, we need to understand reporting is a good thing – may this be reporting things on others or ourselves. The person assigned to manage our insider threat program is the Insider Threat Program Senior Official (ITPSO) **Donald C. Heath, Jr.** The ITPSO develops the program by assigning other key members on the insider threat team and collects the reporting by all of us. The collection of the reporting is reviewed on a periodic basis; the purpose of collecting and reviewing the reports is to identify a possible insider threat situation from developing by thoroughly evaluating the insider threat indicators being reported. Attached to the SPP under 17. References is our Insider Threat

Plan. Annual insider threat awareness is required and some of the reporting conditions are noted under 6. Individual Reporting Responsibilities.

6. Individual Reporting Responsibilities -- SEAD 3 – 117.8

All Tactical Element cleared employees are to report any of the following information listed under this section to the FSO, your main point of contact for reporting. Tactical Element FSO **Donald C. Heath, Jr.** can be reached at 352-459-4186 or dch5657@tacticalelement.com.

Cleared employees will receive the new reporting requirements for additional items under SEAD 3 prior to 1 Mar 2022. Our initial and annual security refresher training has been updated to reflect the new reporting requirements. Under 17. References is a document titled SEAD 3 ISL 2021-02, SEAD 3 Directive and Reporting Slide showing what the new reporting requirements are, additional information about the new SEAD 3 reporting is provided in the initial/annual security training and the actual SEAD 3 Reporting Directive/Industrial Security Letter. The main ways employees will report items outlined under SEAD 3 and any other required reporting requirements due to having a personnel clearance will be either: email or calling the FSO. Another authorized method to report is in person to the FSO.

Tactical Element has an obligation to report items falling into certain categories associated with our cleared work force, part of having a facility clearance and you as a cleared individual having a personnel security clearance (PCL). SEAD 3 requires cleared personnel to report certain items/conditions/situations termed "adverse information" based on the PCL level the person has which is identified in the SEAD 3 ISL 2021-02, SEAD 3 Directive and Reporting Slide and covered in the security training. The term "adverse information" should not be taken negatively, just a term used how to capture one of several reporting categories. As can be seen below, required reporting by cleared personnel falls into the following categories listed from 6.1 – 6.8.

Based on the information being reported and severity of it will determine which category the reporting falls under and then determine what the FSO will do with the report. Example, majority of the information being reportable under SEAD 3 will be recorded in Defense Information Security System (DISS). Depending on the category of information being reported, the information may also be logged by the Insider Threat Program Senior Official (ITPSO) in the database being used for tracking insider threat indicators. The report may also need to be reported to other governmental agencies and our assigned DCSA Counterintelligence Special Agency (CISA)/ISR.

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

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 – 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.

6.3. 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. Reporting on another cleared employee is termed as insider threat reportable indicators. Reportable adverse information includes conditions below and is not an all-inclusive list:

- 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, bankruptcy, 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
- SEAD 3 reportable conditions which many are noted above, see SEAD 3 document under 17. References.
- Foreign travel – unofficial

  The new SEAD 3 reporting requirements now requires all cleared individuals with a personnel security clearance to report foreign travel. Effective August 24, 2022, Tactical Element is required to report your foreign travel in DISS which requires us uploading/answering certain information about your foreign travel. Under 17. References is a form – Foreign Travel Notification, you are required to submit this form when requesting foreign travel. This form must be submitted to your FSO at least 14 days before your foreign travel start date. All deviations from approved travel itineraries shall be reported within five business days of return or sooner.

  - Depending on where you are traveling to, you may want to send in the notification request earlier than 14 days. The FSO will review your form for completeness and may request additional information. Also depending on where you are traveling to, you may be required to get a pre-travel and/or post-travel briefing. Due to all the cyber intrusions and leaks, there have been various governmental databases and our adversaries simply getting better at their tradecraft of espionage, most likely when you are stepping into a foreign country our adversaries know about it. You may be a target, know this and acting accordingly, make sure you report situations that do not seem right to your FSO upon your return. If Tactical Element has contracts requiring individuals to have Special Compartment Information (SCI) and/or Special Access Programs (SAP) access, there may be additional reporting requirements for your foreign travel and where you can travel to. Along with this, there may be other reporting requirements due to being associated with SCI/SAP.
  - Other than submitting the Foreign Travel Notification form, you are required to review the following link before your foreign travel is approved and acknowledged on the request form: https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Safe_Travels.pdf

    Other pertinent links to review are:

    https://www.dvidshub.net/video/854199/sead3-unofficial-foreign-travel-reporting

https://www.dcsa.mil/Portals/91/Documents/CTP/tools/SEAD3_Unofficial_Foreign_Travel_Reporting_and_Activities_Checklist_081022.pdf

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 – 117.8 (d)

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 the 32 CFR NISPOM RULE, this applies to reporting on himself, herself, or another cleared individual. See Section 7 regarding Tactical Element's graduated scale of disciplinary actions.

6.6. Personal Changes

Cleared personnel report personal changes to include:

- Change in name
- 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.

6.8. Insider Threat Reporting

To ensure the protection of classified information or other information specifically prohibited by law from disclosure, cleared individuals at a minimum shall alert the FSO and/or ITPSO to the following reportable activities of other cleared individuals that may be of potential security or counterintelligence (CI) concern, this is not an all-inclusive list on what to report. Throughout history when reviewing insider threat cases, normally there will always be comments by other employees when being interviewed they saw things like noted below but did not report them, saying they did not want to get the person in trouble or thought they were just having a bad day. The reporting conditions below are what security professionals' term as "insider threat indicators". No one wakes up one day and determines they are going to be an active shooter or are going to become a spy that day, history tells us things like this evolve over time with an insider. So, reporting these indicators without judgement may hopefully get the person who is starting to travel down the wrong road the help needed before it gets out of hand.

a. An unwillingness to comply with rules and regulations or to cooperate with security requirements.

b. Unexplained affluence or excessive indebtedness.

c. Alcohol abuse.

d. Illegal use or misuse of drugs or drug activity.

e. 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.

f. Criminal conduct.

g. 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.

h. Misuse of U.S. Government property or information systems.

i. Inappropriate, unusual, or excessive interest in sensitive or classified information

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

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

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

NRC HOTLINE-U.S. NUCLEAR REGULATORY COMMISSION

Office of the Inspector General Mail Stop TSD 28

WASHINGTON, D.C. 20555-0001

TELEPHONE: 800-233-3497

CIA HOTLINE- OFFICE OF THE INSPECTOR GENERAL

Central Intelligence Agency

WASHINGTON DC, 20505

TELEPHONE: 703-874-2600

DOE HOTLINE-DEPARTMENT OF ENERGY

Office of the Inspector General

WASHINGTON DC, 20585

TELEPHONE: 800-541-1625

9. Marking Classified Information – 117.13

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.
- ***CUI*** - ****

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

Tactical Element 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

- ***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

Tactical Element 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 – 117.15 (a) (2)

To ensure that all storage containers are properly secured, the following procedures will be followed at the end of each business day:

10.4. Perimeter Controls

Perimeter controls have been established at Tactical Element to deter and detect unauthorized introduction or removal of classified material. There is a sign conspicuously posted at the front and rear entrances stating that all persons who enter or exit the facility shall be subject to an inspection of their personal effects. All visitors and employees are subject to possible inspection, which will occur at random intervals.

10.5. Receiving Classified Material

All incoming classified material will be received by cleared, authorized individuals.

10.6. Storage of Classified Information

Tactical Element is currently approved to store classified material up to the SECRET level.

Only a minimum number of authorized individuals will have knowledge of the combinations for security containers where classified material is stored. The following procedures apply:

- A record of individuals with access to each container is maintained.
- Containers must be locked when not under direct supervision of an authorized individual.
- All classified material must be secured in the appropriate security container at the end of each working day.

NOTE: Classified information cannot be removed from Tactical Element for use or storage at an individual's private residence.

10.7. Combinations

Authorized persons should memorize the combinations of classified security containers. If a written record of the combination is established, it will be marked and safeguarded in accordance with the highest level of material stored in the container.

Combinations will be changed as soon as possible following:

- The initial receipt of an approved container or lock.
- The reassignment, transfer, termination of any person having knowledge of the combination, or when the security clearance granted to any such person is downgraded to a level lower than the category of material stored, or when the clearance has been administratively terminated, suspended, or revoked.
- The compromise or suspected compromise of a container or its combination, or the discovery of a container left unlocked or unattended.

The combination will be changed by a person authorized access to the contents of the container or by the FSO.

10.8. Transmission of Classified Information

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

10.9. Reproduction of Classified Material

Classified information may only be reproduced on copy machines that have been approved for classified reproduction.

10.10. Destruction of Classified Material

The quantity of classified material on hand will be minimized to the smallest amount consistent with contractual performance. Once classified material has served its purpose, it will be returned to the government customer – or destroyed as soon as possible by:

Classified material will be destroyed at Tactical Element by. Contact the FSO Donald C. Heath, Jr. at 352-459-4186 or dch5657@tacticalelement.com for guidance.

10.11. Retention of Classified Materials

The 32 CFR 117 NISPOM RULE requires classified information provided by the government and any deliverables to be returned at the end of the contract, retention for these items is not authorized. Classified materials created under the contract other than just mentioned may be retained for two years after the conclusion of the classified contract. If retention is needed over two years, retention authority must be requested in writing to the government activity. Contact the FSO for guidance.

11. Public Release/Disclosure – 117.15

Tactical Element 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. The facility clearance granted to our company is not authorized to be used for advertising, such as, posting on our website or in brochures we have a facility clearance.

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

12. Visit Procedures – 117.16

12.1. Incoming Visits

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 the DCSA web-based National Industrial Security System (NISS).

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 Tactical Element 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)

The Information Systems Security Manager (ISSM) maintains System Security Plans (SSP) for all classified information systems. Refer to the SSPs for classified information systems requirements.

NOTE: Classified information CANNOT be entered into any computer or other electronic device at Tactical Element 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 or ISSM.

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.

***Also, Reference 117.8 (c)(9) - Inability to safeguard classified material. The contractor will report any emergency that renders their location incapable of safeguarding classified material as soon as possible.

14.2. Emergency Contact Numbers

Name	Main #	Cell Phone #
FSO	352-459-4186	352-516-7333
SMO	352-459-4186	
ITPSO	352-459-4186	352-516-7333
AFSO	352-459-4186	352-459-5702
ADD Others AS NEEDED		
DCSA		

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 (ENTER FACILITY NAME) employees granted a personnel clearance or who are in process for a personnel clearance.
Closed/Open Area	An area that meets the requirements outlined in the 32 CFR 117 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 in order 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 117 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 117 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 117 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
DoD	Department of Defense
DoD CAF	Department of Defense Central Adjudication Facility
DOE	Department of Energy
DCSA	Defense Counterintelligence and Security Agency
DTIC	Defense Technical Information Center
DISS	Defense Information Security System
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
ISR	Industrial Security Representative
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ITP	Insider Threat Plan
ITPSO	Insider Threat Program Senior Official
ITAR	International Traffic in Arms
KMP	Key Management Personnel
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NISS	National Industrial Security System
NTK	Need-To-Know
OPM	Office of Personnel Management
PCL	Personnel Security Clearance
POC	Point of Contact
PR	Periodic Reinvestigation
S	Secret
SCG	Security Classification Guide
SPP	Standard Practice Procedures
TS	Top Secret
U	Unclassified
US	United States
VRO	Vetting Risk Operations

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] Insider Threat Plan

[7] SEAD 3 ISL 2021-02, SEAD 3 Directive and Reporting Slide SEAD 3 Reporting Requirements

[8] Foreign Travel Notification form

[9] Contractor can provide other References as Needed.