New Mexico Institute of Mining and Technology (NMT)	**Number:** *401*	**Revision:** *3*	**Pages:** *47*
Energetic Materials Research and Testing Center (EMRTC)	**Effective Date:**	**Supersedes:** *SOP 401 dated 25 July 2022*	
Standard Operating Procedure (SOP)	**Sponsoring Function:** *NMT Research Compliance Office & EMRTC Safety & Security Office*		
	Approved By: Cris Clayton **Dr. Cris Clayton Director EMRTC**		

Industrial Security

Periodic Review Completed By		
Name	**Date**	**Signature**

Reasons for Revision/Change

Listed below are the changes included in the revision to this standard operating procedure. Minor changes due to spelling or grammar are not included in this listing:

- New Director at EMRTC 12-9-2025
- Updated to SOP standards based on the NISPOM updates https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117
- New Director at EMRTC 1-4-2024
- Updated to SPP standards based on the CDSE Standard Practice Procedures (SPP) https://www.cdse.edu/Portals/124/Documents/jobaids/industrial/Standard-Practice-Procedures.pdf and
- Security Executive Agent Directive 3- SEAD 3 – Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf
- 32 Code of Federal Regulations (CFR), Part 117, National Industrial Security Program Operating Manual Rule (NISPOM 117). NISPOM 117 https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117
- Industrial Security Letter ISL 2021-02 https://www.dcsa.mil/Portals/91/Documents/CTP/tools/ISL2021-02_SEAD-3.pdf

Table of Contents

1. INTRODUCTION....5
2. SCOPE....5
3. PURPOSE....5
4. RESPONSIBILITY....5
5. ACRONYMS....6
6. DEFINITIONS....6
7. SECURITY EDUCATION NISPOM 117.12....11
7.1 Briefings....12
8. CONTROLLED AREA ACCESS NISPOM 117.15....11
8.1 Visitors....12
8.2 Badges....12
9. RESPONSIBILITIES OF THE SMO & FSO....16
9.1 SMO....17
9.2 FSO....17
10. REPORTABLE ACTIVITIES NISPOM 117.8, SEAD 3, ISL 2021-02....19
10.1 Notifications....19
10.2 Suspicious Contact Reports....19
10.3 Reportable Activities for All Covered Individuals....19
10.4 Reportable Actions by Others....21
10.5 Reportable Activities for Individuals with Access to Secret and Confidential....22
10.6 Reportable Activities for Individuals with Access to TS, "Q" or Special Sensitive Position....22
10.7. Visits by Representatives of Foreign Countries....23
10.8. Public Disclosure....23
10.9. Security Violations....23
11. PERSONNEL CLEARANCE (PCL) PROCEDURES NISPOM 117.10....24
11.1. General Personell Clearance Procedures....24
11.2. TOP SECRET and SECRET Clearances....25
11.3. Changes in Clearance....25
11.4. Debriefing Classified Access....25
12. VISITS NISPOM 117.16....26
12.1 Outgoing Visits....26
12.2. Incoming Visitors....26
12.3. Foreign Visitors....267
13. RECEIPT OF CLASSIFIED MATERIAL NISPOM 117.15....28
13.1. Receiving Classified Packages....28
13.2. Safeguarding and Storing Packages....29
13.3. Classified Material Arriving by CSS or PSS....29
13.4. Accountability of Incoming Classified Documents and Non-Ordnance Hardware....29
13.5. Accountability of Incoming Classified Ordnance....30
14. STORAGE OF CLASSIFIED MATERIAL NISPOM 117.15....30
14.1. GSA-Approved Containers....30
14.2. Opening Lock of GSA-Approved Containers....31
14.3. Logging In: Open / Close GSA-Approved Containers....31
14.4. Closed Areas....31

15. TRANSMISSION OF CLASSIFIED MATERIAL NISPOM 117.15 32
15.1. Modes of Transmission..... 32
15.2. Packaging..... 32
15.3. Courier Procedures..... 33
15.4. Receipts..... 33
15.5. Release or Transmission outside the Facility..... 344
16. REPRODUCTION OF CLASSIFIED MATERIAL NISPOM 117.15 34
17. MARKING CLASSIFIED INFORMATION NISPOM 117.14 34
17.1. Classifying Procedures..... 34
17.2. Incorporating Classified Information into Other Documents 35
17.3. Method of Generation 35
17.4. Working Papers..... 35
17.5. Accountability..... 35
17.6. Satellite Accountability Systems 36
17.7. Test Operations 36
18. MARKINGS NISPOM 117.14 377
18.1 Associate Director of Safety, Security and Environmental Compliance……. 37
19. DISPOSITION OF CLASSIFIED MATERIAL.....37
19.1. Quantity of Material..... 37
19.2. Destruction..... 37
20. RETENTION OF CLASSIFIED MATERIAL NISPOM 117.14 38
21. CONTROL OF AREAS 39
21.1. Duties and Patrols 39
21.2. Closed Area Patrols..... 39
22. EMERGENCY PROCEDURES 39
22.1 Natural Disaster or Civil Disturbance Incapacitates Facility……39
22.2 Riot or Civil Disturbance on NMT Campus…… 40
22.3 Invoking Emergency Procedures…… 40
23. REFERENCES.....40
24. ATTACHMENTS 40
1. Quick Reference Information……41
2. Defense Hotline……42
3. Required Data Elements for Reporting……43

1. INTRODUCTION

This organization is in a security agreement with the Department of Defense in order to have access to information that has been classified due to its importance to National Defense. Many of our programs and activities are vital components of the defense and security of the United States.

All personnel employed by New Mexico Institute of Mining and Technology (NMT) are responsible for properly safeguarding classified information and material.

This Standard Operating Procedure (SOP), also known as a Standard Practice Procedure (SPP), identifies and describes the responsibilities and duties from being a part of our Nation Defense Team. Any employee with questions regarding their security responsibilities should contact the Facility Security Officer (FSO) or alternate FSO (AFSO). All of us have an obligation to see that our security practices are consistent with the best interests of our National Defense Program.

2. SCOPE

This Standard Practice Procedure (SPP) is provided to ensure that New Mexico Institute of Mining and Technology (NMT) and the Energetic Materials Research and Testing Center (EMRTC) meets security requirements in accordance with Code of Federal Regulations (CFR), Part 117, National Industrial Security Program Operating Manual Rule (NISPOM 117).

3. PURPOSE

To provide employees at NMT and tenant organizations with the necessary information to safeguard and protect classified information entrusted to NMT at its various locations and facilities.

4. RESPONSIBILITY

Senior Management Official (SMO): NISPOM 117.7b (1) (iii) and 117.7b (2) Responsible for policy and strategy, the SMO is the ultimate authority over the facility's operations. The SMO appoints the Facility Security Officer (FSO) and Insider Threat Programs Senior Official (ITPSO) and must remain fully informed of the facility's classified operations. The SPP will be signed by the Senior Management Official (SMO) to show management support and make the SPP official.

Facility Security Officer (FSO): NISPOM 117.7b (1) (iii) and 117.7b (3) Supervises and directs the security measures necessary to meet NISPOM and classified contract requirements to ensure the protection of classified information. The FSO will review this SPP every 5 years to ensure it is updated and accurate, consistent with governing documentation and guidance.

Insider Threat Programs Senior Official (ITPSO): NISPOM 117.7b (1) (iii) and 117.7b (4) Establishes and manages the insider threat program.

All personnel assigned to an operation involving classified or sensitive information are responsible for compliance with these procedures.

5. ACRONYMS

ACDA	Arms Control and Disarmament Agency
CAGE	Commercial and Government Entity Number (formerly FSC)
CI	counter intelligence
CSO	Cognizant Security Office
CSS	constant surveillance service
DISCO	Defense Industrial Security Clearance Office
DD	Department of Defense (used to identify forms)
DoD	Department of Defense
DOE	Department of Energy
DSS	Defense Security Service
EMRTC	Energetic Materials Research and Testing Center
EO	Executive Order
FBI	Federal Bureau of Intelligence
FL	form letter
FRS	Field Response Subcommittee
FSO	Facility Security Officer
GCA	Government Contracting Activity
GSA	General Services Administration
LOC	letter of consent
NISPOM	National Industrial Security Program Operating Manual
NMT	New Mexico Institute of Mining and Technology
POC	point of contact
PSS	protective security service
SCR	suspicious contact report
SF	standard form
S&G	Sergeant and Greenleaf
SOP	standard operating procedure
SPP	standard practice procedure
STE	secure telephone equipment
UA	user agency
U.S.	United States
USC	United States Code

6. DEFINITIONS

Access: The ability and opportunity to obtain knowledge of classified information. An individual may have access to classified information by being in a place where such information is kept if the security measures in force DO NOT prevent individuals from gaining knowledge of classified information.

Access Badge: A badge issued to identify personnel who are authorized to access the EMRTC Complex and Field Lab. This badge has the capability to gain the individual access to controlled areas using an access card reader and key pad.

Adverse Information: Information concerning an employee who is currently cleared, or is in the process of being cleared, for access to classified information which reflects adversely upon

the integrity or character of the employee, and could affect his or her ability to safeguard classified information.

Agency: Any "Executive agency" as defined in Section 105 of Title 5, United States Code (U.S.C. Including the "military department," as defined in Section 102 of Title 5, U.S.C., and any other entity within the Executive Branch that come into possession of classified information or has positions designated as sensitive.

Authorized Person: Persons who have a need-to-know for the classified information involved and who have been cleared for receipt of such information. Responsibility for determining whether an individual's duties require that they have access to any classified information and whether they are authorized to receive it, rests upon the individual who has possession, knowledge, or control of the information involved, and not on the prospective recipient.

Automated Information System: an assemblage of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material.

Classified Contract: Any contract that requires, or will require, access to classified information by the contractor or his or her employees in the performance of the contract.

Classified National Security Information or Classified Information: Information or material that is (1) owned by, produced by, or under the control of the United States (U.S.) Government; (2) determined under E.O. 12356 or prior orders to require protection against unauthorized disclosure, and (3) so designated. Information that has been determined pursuant to EO 13526 or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.

Closed Area: A controlled area which meets the requirements of paragraph 5-306 of the NISPOM, as approved by the Cognizant Security Office, for the purpose of safeguarding classified material, which because of its size or nature, cannot be adequately protected by normal safeguards or stored during non-working hours in a GSA-approved container.

Cognizant Security Office: The office of the Defense Security Service (DSS) Director of Industrial Security who has industrial security jurisdiction over the geographical area in which a facility is located.

Cohabitant: A person with whom the covered individual resides and shares bonds of affection, obligation, or other commitment, as opposed to a person with whom the covered individual resides for reasons of convenience (e.g. a roommate).

Compromise: The disclosure of classified information to persons not authorized to access it.

CONFIDENTIAL: The designation applied to information or material, the unauthorized disclosure of which could be reasonably expected to cause damage to the national security.

Controlled Area: An area within an open area deemed "access controlled" because sensitive non-classified material and discussions are in or occur in that area of a facility. Access to this area is controlled with a key lock or a proxy card system allowing only those personnel authorized beyond the control access point to enter.

Controlled Substance: Any controlled substance as defined in 21 U.S.C. 802.

Contractor: Any industrial, educational, commercial, or other entity that has executed a Department of Defense (DD) Form 441, *DoD Security Agreement*, with the DoD for the purpose of performing on a classified contract. The term also refers to an individual who manages such an entity.

Control Point: The location where all traffic enters and exits the Field Lab and is located at the western end of South Road. This location is manned 24-hours a day by Campus Police.

Covered Individual: a. A person who performs work for or on behalf of the executive branch who has been granted access to classified information or holds a sensitive position; but does not include the President or (except to the extent otherwise directed by the President) employees of the President under 3 U.S.C. 105 or 107, the Vice President, or (except to the extent otherwise directed by the Vice President) employees of the Vice President under 3 U.S.C. 106 or annual legislative branch appropriations acts. b. A person who performs work for or on behalf of a state, local, tribal, or private sector entity, as defined in EO 13549, who has been granted access to classified information, but does not include duly elected or appointed governors of a state or territory, or an official who has succeeded to that office under applicable law. c. A person working in or for the legislative or judicial branches who has been granted access to classified information and the investigation or determination was conducted by the executive branch, but does not include members of Congress, Justices of the Supreme Court, or Federal judges appointed by the President. d. Covered individuals are not limited to government employees and include all persons, not excluded under paragraphs (a), (b), or (c) of this definition, who have access to classified information or who hold sensitive positions, including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts, consultants, and government employees.

Custodian: An individual who has possession of, or is otherwise charged with, the responsibility for safeguarding or accounting for classified information.

Documents: Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards, tapes, charts, maps, paintings, drawings, engravings, sketches, working notes and papers; reproductions of such things by any means or process; and sounds, voice, magnetic, or electronic recordings in any form.

Drugs: Any drug as defined in 21 U.S.C. 321.

Espionage: the practice of spying or of using spies, typically by governments to obtain political and military information.

Facility: A plan, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, which, when related by function or location, form an operating entity. For purposes of industrial security, the term does not include User Agency installations.

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).

Field Laboratory (Field Lab): A secured testing area consisting of workshops, ordnance storage magazines, material storage areas and test pad facilities.

Foreign Contact: A foreign national with whom one has continuing contact may be a business/work associate, or someone quite close to you such as a boyfriend, girlfriend, relative's spouse, or family friend.

Foreign Intelligence Entity: Known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.

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 Nationals: Any person who is not a citizen or national of the United States.

Hot Spot: An area/location where political or military tensions are high.

Limited Access Authorization: Security access authorization to CONFIDENTIAL or SECRET information granted to non-U.S. citizens requiring such limited access in the course of their regular duties.

National Security: Those activities which are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, or terrorism.

National Security Eligibility: Eligibility for access to classified information or eligibility to hold a sensitive position, to include access to sensitive compartmented information, restricted data, and controlled or special access program information.

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

Personnel Security Clearance: An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

Representative of a Foreign Interest: A citizen or national of the U.S., or an intending citizen to the U.S. who is acting as a representative of a foreign interest. (See "Foreign Interest.")

Restricted Area: Restricted area means a controlled access area established to safeguard classified material that, because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.

Sabotage: The act of deliberately destroying, damaging, or obstructing (something), especially for political or military advantage.

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

Secured Area:

Sensitive Position: Any position within or in support of an agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on national security regardless of whether the occupant has access to classified information and regardless of whether the occupant is an employee, military service member, or contractor.

Subversive Activity: All willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories of treason, sedition, sabotage, or espionage.

Suspicious Contact Report: Any sort of suspicious contact, foreign travel of our staff (emergency hire, temporary, full time, part time, or students) or visits and contacts from foreign nationals.

Technology Control Plan: A plan used to ensure that no unwanted transfer of classified Department of Defense (DoD) information or controlled unclassified information occurs.

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

Unauthorized Disclosure: A communication, confirmation, acknowledgement, or physical transfer of classified information, including the facilitation of, or actual giving, passing, selling, publishing, or in any way making such information available to an unauthorized recipient.

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

User Agency: Refers to the Office of the Secretary of Defense (including all boards, councils, staffs, and Commands), DOE agencies, Departments of the Army, Navy, and Air Force (including all of their activities), the Departments of State, Commerce, Treasury, Transportation, Interior, Agriculture, Labor, and Justice, and the National Aeronautics and Space Administration, Government Services Administration, Small Business Administration, National Science Foundation, Environmental Protection Agency, Arms Control and Disarmament Agency (ACDA), Government Accountability Office Federal Emergency Management Agency, Federal Response Subcommittee (FRS), United States Information Agency, United States Trade Representative, and United States International Trade Commission.

U.S. Person: An individual, who is not a U.S. Citizen, but who is a lawful permanent resident as defined by 8 United States Code (USC) 11001(a) (20) or who is a protected individual as defined by USC 1324b(a)(3). A U.S. person employed by NMT will not be granted access to sensitive, proprietary or classified information and all export control directives will remain in compliance.

Valid Identification (ID): Refers to government issued credentials (i.e., driver's license, passport, military identification, work visa, etc.)

Visitor Badge: A badge issued to identify personnel who are authorized to access the EMRTC Complex and Field Lab only while being escorted by an individual who possesses an Access Badge and who has been granted escort authorization.

7. SECURITY EDUCATION NISPOM 117.12

Working with classified information makes us a potential target for hostile intelligence interests. Each employee must ensure that classified information within their control is not compromised. Any questions regarding safeguarding classified information should be addressed by the FSO.

Security education may incorporate informational briefings by in-house personnel/special visitors, newsletters, viewing of security-related videos, security quizzes, or the use of other personnel or media.

NMT employees must maintain their awareness that the protection of classified information is vital to our national security. Security violations could endanger the NMT facility security clearance. It is imperative that employees take responsibility for safeguarding of classified information and materials.

7.1. Briefings

7.1.1. **Initial Briefings** will be conducted for each employee following notification from the government that the employee has been granted permission to access classified information.

7.1.2. **Annual Refresher Briefings** will be provided by the FSO to all cleared personnel. This briefing will review the DoD Security Program requirements and your responsibilities as a cleared employee. Employees will receive an annual Threat Awareness Briefing, as well as information on counter intelligence and defensive security measures.

a. Cleared employees will be aware of the security procedures pertaining to their job.

b. Security deficiencies identified during a review will be assessed and preventive/corrective measures will be discussed.

7.1.3. **Periodic Refreshers Briefings** will be provided for foreign travel, special access, and termination from classified access. A record of these briefings will be maintained by the FSO.

8. CONTROLLED AREA ACCESS NISPOM 117.15

EMRTC has two controlled areas within its property; the controlled area within the EMRTC Complex and the secured Field Laboratory (Field Lab). Only NMT employees, student hires, staff, tenants, visitors who have official business or individuals who have permission from the EMRTC Director may enter these areas. Unless otherwise specified, all personnel entering a controlled area must be issued and wear an access badge. Badges must be visibly displayed at all times when in a controlled area. EMRTC complex will be secure 24 hours a day and all authorized individuals must use their proxy badge to enter.

8.1. Visitors

8.1.1. Visitors on official business are required to sign in at Visitor Control before being issued an access badge to enter controlled areas. Information required includes:

- Name

- Company
- Point of Contact (POC)
- Contact Phone Number
- Area visiting

8.1.2. Visitors entering a controlled area must sign in at Visitor Control, be issued a visitor badge, and be escorted at all times when in the controlled area.

8.1.3. Visitors are required to show valid identification (ID) before being issued an access badge.

8.1.4. The visitors escort, or POC, will be notified of the visitor's arrival and will be requested to come to Visitor Control to escort the individual(s) to their desired location.

8.1.5. Escorts will be responsible for badges to include returning the badge to Visitor control upon completion of visit.

8.1.6. Visitor Control should be immediately notified of any lost or stolen badges.

8.2. Badges. Badges are required to be worn by all personnel who are entering a controlled area (i.e., EMRTC complex secured area or Field Laboratory) unless they meet the exception stated in the following note.

8.2.1. All lost or stolen badges will be reported immediately to Visitor Control

NOTE
Visitors associated with a class (i.e., First Responders, NMT courses, etc.) or individuals involved in special events are not required to be issued badges or be signed in at Visitor Control as long as they are within the control of an individual(s) with escort privileges at all times.

8.2.2. *Visitor Badges*

a. **ESCORT REQUIRED** (Pictured badge with orange border)
- Must be associated with a test or project exceeding 5 work days. Less Than 5 days, receives a non-pictured visitor badge.
- Must sign in at Visitor Control prior to being issued badge.
- Must provide valid ID.
- Must be escorted within the controlled area at all times.
- Cannot drive in the Field Lab unless they are being escorted by an individual with escort privileges. If escort is in a separate vehicle, the escort vehicle must be in front of, or leading the visitor's vehicle.
- Must return access badge to Visitor Control upon expiration date.
- At initial check-in, the visitor has an option if engineer/point of contact requests, of being signed in to a specific site for a period of not to exceed 5 days within a consecutive calendar week. The visitor will then report daily for check-in/check-out within the reported period to their POC/escort. Visitor Control must document this arrangement into the Visitor Control log.

b. **UNESCORTED** (Pictured badge with green border)

- Must be associated with a test, project, or service exceeding 5 work days, or be a subcontractor (e.g., utility company) with a need for unescorted access.
- Must return access to badge to Visitor Control upon expiration date.
- Must provide a letter requesting unescorted access to the Field Lab on form provided by NMT Visitor Control.
- Must sign in at Visitor Control prior to entry of Field Lab and upon exit of Field Lab unless access is needed after normal duty hours.
    - Campus Police will log in and out individuals needing access to the Field Lab after hours.
    - At initial check-in, the visitor has an option if engineer/point of contact requests, of being signed in to a specific site for a period of not to exceed 5 days within a consecutive calendar week. The visitor will then report daily for check-in/check-out within the reported period to their POC/escort. Visitor Control must document this arrangement into the Visitor Control log.
- Must provide valid ID.
- Must have attended the Field Lab Safety Briefing.
- All NMT employees and NMT students must have a valid Defensive Driving Certificate (DDC).
- Must possess a valid government issued driver's license with applicable endorsements if driving a vehicle that requires Department of Transportation endorsements.
- **By accepting an unescorted badge, the individual is acknowledging that they have experience being in the Field Lab and are comfortable with the warning system and EMRTC procedures.**

c. **Foreign Nationals – ESCORT REQUIRED** (Pictured badge with yellow border)

- ALL Foreign Nationals WILL be issued a pictured badge during their visit unless they meet any of the special circumstances mentioned in section 11.3.
- Foreign Nationals will provide valid ID for internal records. Copies of such documents will be made and logged in the Foreign National Log Book.
- Foreign Nationals are required to return access badges to Visitor Control, or their escort if Visitor Control is not available, at the end of each day unless other arrangements have been made.

8.2.3. *Employee Badges*

a. **UNESCORTED – <u>EMRTC Building Access Only</u>** (proxy badge with picture without E)

- Employed by NMT (full time, part time and emergency hires).
- Student Hires (access restricted to 8am to 5pm, Monday through Friday unless otherwise approved by their supervisor, Safety and Security offices or the EMRTC Director).

b. **UNESCORTED – EMRTC Complex and Field Lab Access** (proxy badge with picture with E)
    - Employed by NMT (full time, part time and emergency hires).
    - Student Hires (access restricted to 8am to 5pm, Monday through Friday unless approved by their supervisor, Safety and Security offices or the EMRTC Director).
    - Must have attended the Field Lab Safety Briefing.
    - All NMT employees and NMT students must have a valid DDC.
    - Must possess a valid government issued driver's license with applicable endorsements if driving a vehicle that requires Department of Transportation endorsements.
    - **By accepting an unescorted badge, the individual is acknowledging that they have experience being in the Field Lab and are comfortable with the warning system and EMRTC procedures.**

8.2.4. *Temporary Badges*

a. **ESCORT REQUIRED** (Numbered orange badge with no picture and signed by Senior Safety Officer)
    - Used for short visits by non-employees (5 or less work days).
    - Visitors must sign in at Visitor Control.
    - Visitors must provide valid ID.
    - Must be escorted within controlled areas at all times.
    - Cannot drive in Field Lab unless being escorted by an individual with escort privileges (if visitor is in separate vehicle, the escort vehicle must be in front of, or leading, the visitor's vehicle).
    - Must return access badge to Visitor Control at the end of the day or when departing EMRTC, whichever comes first.
    - Escort is responsible for returning assigned temporary badge.
    - At initial check-in, the visitor has an option if engineer/point of contact requests, of being signed in to a specific site for a period of not to exceed 5 days within a consecutive calendar week. The visitor will then report daily for check-in/check-out daily within the reported period to their POC/escort. Visitor Control must document this arrangement into the Visitor Control log.

b. **UNESCORTED** (Numbered green badge with no picture)
    - Used for employees or student hires who have forgotten or lost their assigned badge.
    - Must sign in at Visitor Control to receive badge.
    - Must return access to badge to Visitor Control at the end of the day or when departing EMRTC, whichever comes first.

Figure 7.2.1- 7.2.2 – Badge Examples



Figure 7.2.2.3 – Badge Example

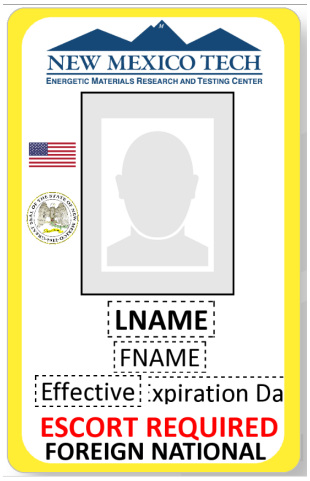


Figure 7.2.3 – Badge Example

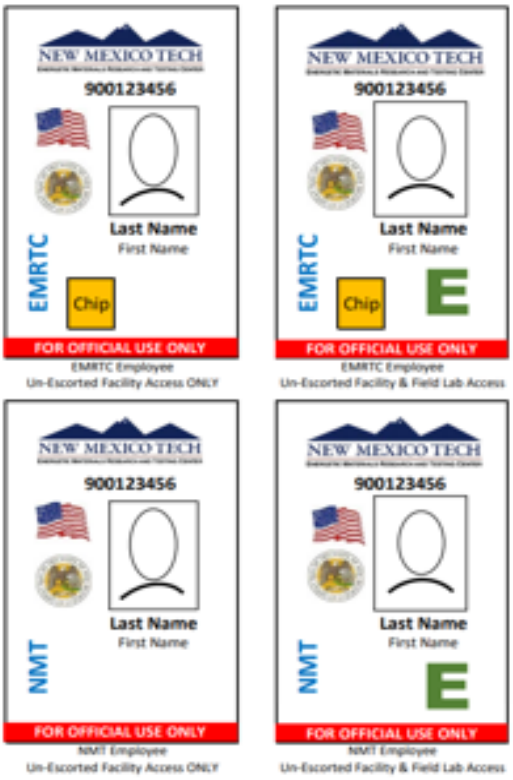


Figure 7.2.4.1 – 4.2.4.2 – Temporary Badge Examples



9. RESPONSIBILITIES OF THE SMO & FSO

9.1. The NMT SMO, NISPOM 117.7b (1)

9.1.1. (i) The SMO is the contractor's official responsible for the entity policy and strategy. The SMO is an entity employee occupying a position in the entity with ultimate authority over the facility's operations and the authority to direct actions necessary for the safeguarding of classified information in the facility. This includes the authority to direct actions necessary to safeguard classified information when the access to classified information by the facility's employees is solely at other contractor facilities or USG locations

9.1.2. SMO:

a. Ensures the contractor maintains a system of security controls in accordance with the requirements of this part.

b. Appoint a contractor employee or employees, in writing, as the FSO and appoint the same employee or a different employee as the ITPSO. The SMO may appoint a single employee for both roles or may appoint one employee as the FSO and a different employee as the ITPSO.

c. Remain fully informed of the facility's classified operations.

d. Make decisions based on classified threat reporting and their thorough knowledge, understanding, and appreciation of the threat information and the potential impacts caused by a loss of classified information.

e. Retain accountability for the management and operations of the facility without delegating that accountability to a subordinate manager.

9.2. The NMT FSO, NISPOM 117.7b (1) (iii) and 117.7b (3) is responsible for administering the security program under the direction of the SMO of New Mexico Tech. NISPOM 117.7b (1) (iii) and 117.7b (2) and will perform the following functions:

9.2.1. FSO:

a. Monitor the effectiveness of reporting requirements and develop recommendations for or modified requirements.

b. Oversee agency compliance.

c. Ensure best practices are identified, shared, and implemented.

d. Develop reporting guidance and processes that include the Required Data Elements for Reporting, in Attachment 3.

c. Automate and centralize reporting to the extent practicable.

d. Maintain all reported information consistent with applicable law and policy.

e. Ensure policies and procedures governing the collection and use of reported information are in accordance with all applicable laws and executive orders and include appropriate protections for privacy and civil liberties.

f. Analyze, act upon, and share, as appropriate, relevant reported information of a security, counterintelligence (CI), or law enforcement concern with authorized security, CI, insider threat, or law enforcement officials.

g. Share relevant reported information that may result in an adverse determination of the covered individual's continued national security eligibility with security or CI officials of other agencies that have a direct interest in the covered individual. Direct interest is defined as the covered individual being on joint duty, detail, or otherwise working for or within the other agency; or the other agency has granted access or additional access to the covered individual.

h. Provide training and briefing to include ensuring awareness of individual reporting obligations, at a minimum, during employee indoctrination and in annual refresher training.

i. Receive, prepare, and submit reports. Strict attention will be given to the correct routing when submitting reports. Reports concerning the following will be reported to the Cognizant Security Agency:

- Adverse information,
- Suspicious contacts,
- Change in cleared employee status,
- Citizenship by naturalization,
- Employees desiring not to perform on classified work,
- Refusal of employee to fill out a Standard Form (SF) 312, *Classified Information Nondisclosure Agreement,*
- Change conditions affecting the facility clearance,
- Changes in storage capability,
- Inability to safeguard classified material,
- Security equipment vulnerabilities,
- Unauthorized receipt of classified material,
- Employee information in compromise cases,
- Disposition of classified material terminated from accountability, and/or
- Foreign classified contracts.
- Reports regarding information coming to NMT's attention concerning the following will be sent to the Federal Bureau of Investigation (FBI):Actual, probable or possible espionage,
- Sabotage,
- Terrorism, or
- Subversive activities at any of its locations.

j. Maintain all facility clearance records, including Defense Security Service (DSS) Form Letter (FL) 381-R, *Letter of Notification of Facility Security Clearance,* and DD Form 441 or 441-1, *DoD Security Agreement*.

k. Maintain all personnel security clearance records including training certificates and records of briefings.

l. Maintain the NISPOM 117, National Industrial Security Program Operating Manual Rule (NISPOM).

m. Prepare a listing of all classified contracts on which NMT is currently performing work on for upcoming security inspections by the Government.

n. Instruct all cleared employees as to their individual responsibilities for safeguarding classified information and to execute an SF 312, *Classified Information Nondisclosure Agreement,* in order to obtain a clearance and terminate a clearance.

o. Debrief and remove access.

p. Prepare and process clearance requests.

q. Implement a self-inspection program in order to evaluate all security procedures applicable to NMT. The security program will be subject to continuous review, and a formal self-inspection will be conducted approximately midway between scheduled Government inspections.

r. "Work with the EMRTC Senior Safety & Security Officer to Implement a plan of perimeter controls to prevent employees and visitors from introducing or removing classified material from facilities without authorization by the FSO.

10. REPORTABLE ACTIVITIES NISPOM 117.8, SEAD 3, ISL 2021-02

10.1. Notifications

10.1.1. Cleared employees must report instances of espionage, compromise, and adverse information to the FSO immediately, but not later than the next duty day.

NOTE
Additional notifications to appropriate management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.

10.1.2. Consult with the FSO if there is doubt of whether an incident would be considered an act of espionage, compromise, or adverse information.

10.1.3. An inquiry will be conducted by the FSO, or other designee, to determine the cause and effect of the incident and the suitability of administrative or disciplinary action against the offender.

10.2. Suspicious Contact Reports

10.2.1. All suspicious contact reports (SCR) are transmitted to DoD Counter Intelligence (CI) Office. The CI office will reply with a SCR number assigned to the report. All SCR replies from the DoD CI are printed and maintained for DSS review.

10.3. Reportable Activities for All Covered Individuals

10.3.1. **Foreign Travel**

- All foreign business or personal travel (vacation, family emergency, etc.) will be reported in advance (at least 3 weeks before) to the FSO so they can schedule a CI briefing.

- Report all foreign travel in advance where a pre-travel defensive security briefing would be requested or required or if travel is to a "Hot Spot" country, region, or area. Contact the FSO if you're unsure if the country in questions is a "Hot Spot."
- A post-briefing with the FSO will be conducted upon the return from any foreign travel.

1) Covered individuals shall submit an itinerary for unofficial foreign travel to the FSO or designee and, except as noted in the subparagraphs below, must receive approval prior to the foreign travel. 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 within five business days of return.

a) Travel to Puerto Rico, Guam, or other U.S. possessions and territories is not considered foreign travel and need not be reported.

b) Unplanned day trips to Canada or Mexico shall be reported upon return. Reporting shall be within five business days.

c) When required by the agency head or designee, covered individuals shall, prior to travel, receive a defensive security and counterintelligence briefing.

d) 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, with the SFO, prior to departure. In any event, full reporting shall be accomplished within five business days of return.

e) Consistent with national security, the SFO 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.

2) The FSO 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.

10.3.2. **Foreign Contacts**

- Any attempt Any attempt by a foreign national to solicit sensitive or classified information or any other contact that you regard as suspicious.

- Close and continuing contact with a foreign national in any capacity; in person, by telephone, via internet, etc.
- Contact with anyone who works for, or is associated with, a foreign government (including a foreign embassy), or a foreign-owned organization or business. Financial obligations regarding investments or employment with foreign nationals and companies.

a. The FSO or designees shall determine requirements for reporting contact with a foreign national as part of a covered individual's official duties.

b. Unofficial Contacts:

1) Unofficial contact with a known or suspected foreign intelligence entity.

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. 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.). The reporting of limited or casual public contact with foreign nationals is not required absent any other reporting requirement in this directive. Following initial reporting, updates regarding continuing unofficial association with known foreign nationals shall occur only if and when there is a significant change in the nature of the contact. Heads of agencies or designees may provide specific guidance and examples of updated reporting situations.

10.4. Reportable Actions by Others:

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

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. Covered individuals who have been identified by the FSO in accordance with EO 12968, as amended, Section 1.3. (a) shall file a financial disclosure report, as appropriate.

NOTE
Use of medical marijuana is prohibited by cleared personnel

10.5. Reportable Activities for individuals with access to Secret and Confidential Information, “L” Access or holding a Non-Critical Sensitive Position:
In addition to the reporting requirements in Sections 10.3 and 10.4, individuals with access to Secret and Confidential information, "L" access, or holding a Non-Critical sensitive position shall also report:

1. Foreign Activities:

a. Application for and receipt of foreign citizenship.

b. Application for, possession, or use of a foreign passport or identity card for travel.

2. Other Reportable Activities:

a. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of means.

b. Media contacts, other than for official purposes, where the media seeks access to classified information or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure. Media contacts related to the fulfillment of official duties of the position held by the covered individual need not be reported.

c. Arrests.

d. Bankruptcy or over120 days delinquent on any debt.

e. Alcohol-and drug-related treatment.

10.6. Reportable activities for individuals with access to Top Secret, “Q” Access, or holding a Critical or Special Sensitive position. In addition to the reporting requirements in Section 10.3 and 10.4, individuals with access to Top Secret information, "Q" access, or holding a Critical or Special sensitive position shall also report:

1. Foreign Activities:

a. Direct involvement in foreign business.
b. Foreign bank accounts.
c. Ownership of foreign property.
d. Application for and receipt of foreign citizenship.
e. Application for, possession, or use of a foreign passport or identity card for travel.
f. Voting in a foreign election.
g. Adoption of non-U.S. citizen children.

2. Other Reportable Activities

a. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of means.
b. Media contacts where the media seeks access to classified information or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure. Media contacts related to the fulfillment of official duties of the position held by the covered individual need not be reported.
c. Arrests.
d. Financial Anomalies: Including, but not limited to, bankruptcy; garnishment; over 120 days delinquent on any debt; and any unusual infusion of assets of $10,000 or greater such as an inheritance, winnings, or similar financial gain.
e. Foreign National Roommate(s): Any foreign national(s) who co-occupies a residence for period of more than 30 calendar days.
f. Cohabitant(s).
g. Marriage.
h. Alcohol- and drug-related treatment.

10.7. Visits by Representatives of Foreign Countries

10.7.1. FSO must be notified of plans to host a visit by representatives of a foreign country at least 3 weeks prior to the visit unless prior arrangements have been made.

10.7.2. The FSO must be provided with a copy of the foreign national's passport(s) at least 5 days prior to the visit so that it can be vetted through the Defense Security Service unless prior arrangements have been made. See Section 11.3. Foreign Visitors.

10.8. Public Disclosure

10.8.1. The fact that the information currently classified has been disseminated by a public medium of communication does not automatically mean it has been declassified. To assure that classified information furnished or released only to authorized persons, public disclosure of information pertaining to classified information shall be in accordance with security requirements received from the contracting officer.

10.9. Security Violations

10.9.1. **Report all violations** that directly involve the mishandling of classified information, and if a cleared or in-process individual can be identified.

10.9.2. **Reports may be made** for violations which did not directly involve the mishandling of classified information, yet represents a deliberate disregard for security requirements. It is required that on-the-spot corrections be made for these types of violations.

10.9.3. **Non-deliberate security violations** may be reported as adverse information only if they indicate a pattern of negligence or carelessness.

a. **First violation** within a period of 12 consecutive months: Issuance of a security awareness letter, counseling by the FSO and the Director of EMRTC, and any other corrective or disciplinary action deemed appropriate by an appointed committee.

b. **Second violation** within a period of 12 consecutive months: Written reprimand and any other corrective or disciplinary action deemed appropriate by an appointed committee. Disciplinary action could include leave without pay in accordance with the NMT Employee Handbook.

c. **Third violation** within a period of 12 consecutive months: Disciplinary suspension and any other corrective or disciplinary action deemed appropriate by an appointed committee. Disciplinary action could include termination of employment in accordance with the NMT Employee Handbook.

d. **Incident Reports** for all violations will be submitted to DCSA (https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Facility-Clearances/Maintaining-Personnel-Security-Clearances/)

e. FSOs will submit reports for personnel with a security clearance, in-process for a clearance, or a that have a clearance eligibility that could be reinstated, in accordance with the reporting requirements in paragraph 1-302 of the National Industrial Security Program Operating Manual (NISPOM). DISS provides the incident report capability to facilitate this reporting. At this time, the FSO will mark report as "final" rather than "initial".

11. PERSONNEL CLEARANCE (PCL) PROCEDURES NISPOM 117.10

11.1. General

11.1.2. New requests for clearance processing will be reviewed by the Director and will be approved by the FSO.

11.1.3. Requesting Supervisor will provide the FSO with notification indicating the need for an employee to obtain a clearance

11.1.4. Employee will provide the FSO evidence to verify US Citizenship. A record will be made of which documents were cited as proof of citizenship.

11.1.5. The following documents are acceptable as proof of citizenship:

- Birth Certificate

- Certificate of naturalization
- Certificate of citizenship
- Passport (current or expired)
- Record of military processing (DD Form 1966)

11.2. TOP SECRET and SECRET Clearances

11.2.1. TOP SECRET and SECRET will accurately complete the Standard Form-86, "Questionnaire for National Security Positions" (available at *https://www.opm.gov/forms/pdf_fill/sf86.pdf*), which applicants and clearance holders complete during the initial and Continuous Vetting (CV) processes. Every employee with access will fill out an SF86 every five years regardless of PCL level.

11.2.2. The FSO will inform the employee in writing that the SF86 review is only for adequacy and completeness and no other purpose within the company. Fingerprints are submitted with the PCL application.

11.2.3. NISPOM Paragraph 3-106 requires that an individual issued an initial personnel security clearance (PCL) execute a Classified Information Nondisclosure Agreement (SF-312) prior to being granted access to classified information and that the completed form is forwarded to the Cognizant Security Agency for retention. The Facility Security Officer (FSO) is responsible for uploading the signed SF-312 into the DISS application.

11.2.4. Employees who have not had access to classified information within six (6) months will have their access removed. The FSO will evaluate all clearances on a quarterly basis to determine compliance.

11.3. Changes in Clearance

11.3.1. Cleared personnel or their Supervisor will report any of the following to the FSO:

- Termination of employment
- Retirement or death of an employee
- Transfer to another division
- Administrative downgrading
- Change in name
- Change in employment status

11.3.2. The security office will notify the CSA through DISS of any of these changes.

11.4. Debriefing Classified Access

11.4.1. Whenever clearances are no longer needed (i.e. employee goes on workman's compensation, takes a leave of absence, employment is terminated, etc.), PCL employees are required to be debriefed. NISPOM 117.12

11.4.2. Administratively terminated clearances may be re-validated within 24 months of the administrative termination, provided the employee was continuously employed at NMT and if the need for the clearance still exists.

12.VISITS NISPOM 117.16

The number of classified visits will be held to a minimum and approved in advance. Determine if the visit is necessary and cannot be achieved without access to, or disclosure of, classified information. Establish procedures to ensure positive identification of visitors, appropriate PCL, and need-to-know prior to the disclosure of any classified information. Only afford classified access consistent with the purpose of the visit. For outgoing classified visits, provide company FCL and employee PCL information, the name of the person to be visited, the time and duration of the visit, and the justification for the visit. Process outgoing visits in the database of record or by submitting a Visit Authorization Letter (VAL) document.

12.1. Outgoing Visits

12.2.1. When cleared NMT employees need to access classified information at other cleared contractor facilities, User Agency (UA) activities, or installations, the following procedures apply:

a. The Employee will complete an outgoing visit request, and submit it to the FSO.

b. The FSO will be notified of the contractor or UA to be visited, the time and duration of the visit, the reason for the visit, and the person to be contacted.

c. A visit request will be prepared by the FSO in accordance with the NISPOM.

d. In the event that a visit must be processed on extremely short notice, the FSO may contact the host facility by telephone and request verbal approval for the visit; the FSO will provide the visitors' name, social security number, date and place of birth, citizenship, and will submit a written visit request within 24 hours.

e. A visit request may be submitted for specific dates or for the whole period of the visit, but will not exceed 12 months.

f. If a cleared employee dies, terminates employment, transfers, retires, or no longer requires access under an existing visit request, the FSO must cancel all outstanding visit requests in writing.

12.3. Incoming Visitors

12.3.1. The FSO or Alternate FSO will review all incoming visit requests before allowing access to classified information in any form.

12.3.2. All visitors who require access to classified information must have both a personnel security clearance at the appropriate level, as well as a need-to-know for the classified information involved.

12.3.3. The point of contact (POC), or designated representative, will notify the FSO or Alternate FSO of visitors who are here on a classified visit before entry into the visit request system.

12.3.4. The visitors' POC will establish proper visit requests and ensure that a level of clearance has been established before requesting visitor's access to classified

information. Visitors will not be given access to classified information without having a valid clearance or permission to discuss or witness a particular project.

12.3.5. The contracting officer will be asked to certify the need-to-know before release of data to the visitor, should any visit or request specify a discussion of information on material outside the requesting agency's authorization.

12.3.6. If NMT has a contractual relationship that involves classified information with a private company, then the requirements discussed above will be followed for visitors from that company.

12.3.7. If NMT receives a visit request from a company with whom it does not have a classified contractual agreement, the following must be verified:

- Company has the authority to issue a visit request; and
- Company has a need-to-know.

12.3.8. Visits by Industrial Security representatives of the DoD, other UAs, and representatives of the following Government agencies, when acting in their official capacities, may visit contractor facilities without furnishing advanced notification:

- Defense Security Service
- DoD Inspector General, Defense Criminal Investigative Service
- U.S. Army Intelligence and Security Command
- Naval Investigative Service
- U.S. Air Force, Office of Special Investigations
- Secret Service
- Federal Bureau of Investigation
- General Accounting Office
- Department of Labor
- National Security Agency, Central Office of Record

12.4. Foreign Visitors

12.4.1. These procedures apply to all visits by foreign nationals. This includes visits which are classified, unclassified, official or unofficial.

NOTE

In the event of Public or Special Events, the FSO and/or AFSO will prepare a plan for risk mitigation. The foreign nationals attending the event will not be required to be badged or show identification. In place of formal vetting, the FSO, or designee, will provide briefings to escorts and volunteers involved in the event on suspicious activities, contacts, and reportable incidents. All individuals participating in these events will be monitored to ensure there is no disclosure of export controlled, proprietary, or classified information or technical data. The FSO, or designee, will be involved in the event to provide oversight and monitoring.

12.4.2. The sponsor, or POC, of the visitor must inform the FSO of pending UNCLASSIFIED visits no later than five (5) days and CLASSIFIED visits no later than ten (10) days prior to the actual visit in order to conduct necessary

government vetting through the Department of State will be performed for all CLASSIFIED visits.

12.4.3. The following information must be provided to the FSO:

- Visitor's name, title, company, date of visit, and purpose of the visit.
- Copy of a valid ID.

12.4.4. The FSO or AFSO is responsible for contacting the NMT Export Control Program Specialist to inform them of the visit.

12.4.5. The FSO and/or AFSO will report the visitors to DISS as a Suspicious Contact Report.

12.4.6. All escorts will be debriefed after completion of escort duties by the FSO or designee.

12.4.7. Upon the visitors' arrival, the visitor and the visitors escort will be given the Technology Control Plan (TCP) briefing and they will be asked to sign a briefing acknowledgement form stating they have been briefed and understand the content of the briefing.

12.4.8. Visitors will be issued a Foreign National Visitor Badge from Visitor Control, in accordance with 7.3.2.3, and will be required to wear it at all times while at any EMRTC facility.

12.4.9. Visitors will be escorted at all times.

13. RECEIPT OF CLASSIFIED MATERIAL NISPOM 117.15

13.1. Receiving Classified Packages

13.1.1. New Mexico Tech is approved to receive classified packages ONLY via Federal Express.

13.1.2. The shipping address for the receipt of classified materials destined for EMRTC and/or ICASA is:

New Mexico Tech / EMRTC
Attention: Document Control
1001 South Road
Socorro, NM 87801

13.1.3. A classified (or potentially classified) package will arrive via Federal Express. A cleared, authorized individual will sign for and receive the package from the Federal Express driver. **Do Not** make any indication that the package may or may not be classified. Keep the package in constant surveillance until it is secured by EMRTC Security Office personnel.

13.1.4. Note the address on the package. If there is any indication that the package is classified, contact the New Mexico Tech FSO or Alternate FSO immediately to take possession of the package.

13.2. Safeguarding and Storing Packages

13.2.1. If you are unable to locate or contact a member of the EMRTC Security Office, place the package in the Government Services Administration (GSA)-approved container located in the EMRTC Warehouse.

13.2.2. When the appropriate EMRTC Security personnel are notified, open the container and provide the package to the EMRTC Security Office.

13.3. Classified Material Arriving by CSS or PSS

13.3.1. Hardware or hazardous material classified CONFIDENTIAL is received via an approved carrier that provides protective Constant Surveillance Service (CSS).

13.3.2. Hardware or hazardous material classified TOP SECRET or SECRET is received via an approved carrier that provides Protective Security Service (PSS).

13.3.3. Items that are either too big or too hazardous to be handled at the EMRTC office will be received and signed for by an authorized individual.

13.3.4. A copy of the receiving papers will be delivered to the FSO after they have been stored in approved closed areas in the Field Laboratory.

13.3.5. Procedures for receiving classified material will be followed and brought into accountability. At that time, the shipment will be assigned a control number and will be included in the Classified Inventory List.

13.4. Accountability of Incoming Classified Documents and Non-Ordnance Hardware

13.4.1. Documents and non-ordnance hardware will be assigned an Accountability Number.

13.4.2. These item(s) will be entered in the Classified Inventory Listing and will include the following information, as applicable:

- Accountability number,
- Date received,
- Issuing agency,
- Author,
- Unclassified title or description of the material,
- Date of publication, Declassification or downgrading instructions,
- Contract number received under, and
- Disposition (location to be stored).

13.4.3. The item(s) will be inspected for proper markings, and if documents have been inserted in a file folder that has been stamped with the level of classification on both front and back, marked with the control number and entered into the Security Information Management System.

13.4.4. All TOP SECRET and SECRET material will arrive with receipts that must be signed, dated, and returned to the sender.

13.4.5. If a return receipt is included with CONFIDENTIAL material, it must be signed, dated and returned.

13.5. Accountability of Incoming Classified Ordnance

13.5.1. All shipments involving classified ordnance will be unloaded, inspected, inventoried, and stored in appropriate magazines.

13.5.2. Items will be assigned an Accountability Control Number, based on their storage magazine, and a sequential number as described in section 12.4.

13.5.3. The recipient will sign any receipts arriving with the classified ordnance. If a receipt is not with the ordnance, check to see if the driver has the receipt.

13.5.4. All receipts and other paperwork will be hand carried to the FSO, with verification of the shipment's contents, for signature and return to the shipper.

14.STORAGE OF CLASSIFIED MATERIAL NISPOM 117.15

All TOP SECRET, SECRET and CONFIDENTIAL material will be stored in a GSA-approved container, or within an approved closed area. The FSO will maintain a list of all GSA-approved containers and closed areas.

14.1. GSA-Approved Containers

14.1.1. Storage of classified material at a private residence is NOT authorized.

14.1.2. Only the minimum number of authorized persons will have access to GSA-approved containers and closed areas.

a. A record of the names of personnel having knowledge of the combinations will be maintained in the Security Office.

b. GSA-approved containers and areas will be kept locked when not under the direct supervision of authorized personnel.

14.1.3. Authorized personnel will be required to memorize combinations for each GSA-approved container with a combination lock.

14.1.4. The FSO will maintain a written record of all combinations. All combinations will be changed under the following circumstances:

a. The initial receipt of a GSA-approved container, or three-position combination padlock.

b. The reassignment, transfer, or termination of any person having knowledge of the combination, or when the security clearance granted to any such person is administratively terminated, suspended or revoked by proper authority.

c. The compromise or suspected compromise of any combination or the discovery of a GSA-approved container having been unlocked and unattended; or,

d. At other times when considered necessary by the FSO.

14.1.5. Only the FSO or a designated representative may change combinations.

14.2. Opening Lock of GSA-Approved Containers

14.2.1. **Combination**

a. The combination for opening the GSA-approved container will be provided to the cleared employees who have been granted access to the GSA-approved container.

b. The combination shall not be written or stored in any fashion. Instead, the GSA-approved container combination must be memorized and not recorded.

c. Training will be provided by the EMRTC Security Office on the method to operate the combination lock of the GSA-approved container.

14.3. Logging In: Open / Close GSA-Approved Containers

14.3.1. **Security Container Check Sheet**

a. A Security Container Check Sheet will be provided by the EMRTC Security Office and used to log all open / close operations of GSA-approved containers.

b. The Security Container Check Sheet is located on the top of the container. Document the date and time the container was opened and initial the Check Sheet. Note the time the container was closed and initial the Check Sheet.

c. End-of-day checks will be conducted daily, whether the GSA-approved container was opened or not. If the GSA-approved container remained unopened that day, note on the Check Sheet "Not Opened" and identify the date and time of the check. Initial next to date and time.

d. Always notify the EMRTC Security Office if there are no cleared EMRTC personnel available to conduct an end-of-day check. The EMRTC Security Office will perform the end-of-day check in the absence of EMRTC cleared personnel.

e. NEVER leave the container unattended while open.

f. If at any time you arrive to an open container and find it unsecure and unattended, you must immediately notify the FSO or Alternate FSO.

g. If you cannot locate the FSO or Alternate FSO, contact EMRTC Visitor Control and request that Visitor Control immediately contact the EMRTC Security Office.

h. Immediately contact New Mexico Tech Campus Police if you cannot locate an EMRTC Visitor Control staff member.

i. A transmittal receipt must accompany each classified shipment. The receipt will identify the classified contents, as well as the name and address of the sending and receiving facilities.

14.4. Closed Areas

14.4.1. Closed areas will be locked with either a Sargent and Greenleaf (S&G) combination or 831B high security lock.

14.4.2. All locks and keys used to secure classified will be audited monthly.

14.5. The appropriate security custodian will conduct end-of-day security checks. These checks will, at a minimum, verify that all classified material at each location has been secured, and that all containers are security locked.

15.TRANSMISSION OF CLASSIFIED MATERIAL NISPOM 117.15

15.1. Modes of Transmission

15.1.1. TOP SECRET and SECRET material may be shipped only by:

- U.S. Postal Service (USPS) Express Mail,
- USPS Registered Mail,
- Cleared commercial carrier,
- Cleared commercial messenger service engaged in the intercity/local area delivery (same day delivery only) of classified material, or a
- Commercial Delivery Company approved by the CSA.

15.1.2. CONFIDENTIAL material may be transmitted by USPS Certified Mail, or the same methods as SECRET material, except that a commercial carrier does not have to be cleared.

15.1.3. **Shipping by Commercial Carrier**

a. Classified hardware can be shipped by commercial carrier only when the size, bulk, weight, nature of shipment, shipping costs, or escort considerations make use of the USPS impractical.

b. The carrier must be Government licensed and able to provide CSS for CONFIDENTIAL materials and PSS for TOP SECRET and SECRET materials. A list of approved carriers will be maintained in the EMRTC Security Office.

c. Containers must be of such strength and durability that the contents are not likely to break out. The Bill of Lading must indicate that CSS or PSS is required. Carrier must be instructed to ship packages weighing less than 200 pounds in a closed vehicle or a closed portion of the carrier's equipment.

d. The consignee must be notified by telephone at least 24 hours in advance (or immediately upon dispatch if transit is less than 24 hours) of the arrival of the shipment in order that the consignee may take appropriate steps to receive and protect the shipment.

e. It is advised that the consignor notify EMRTC of any shipment not received within 48 hours after the estimated time of arrival.

15.2. Packaging

15.2.1. The classified material and transmittal receipt will be packaged in opaque inner and outer containers.

15.2.2. The inner container will be addressed, return addressed, and marked on all sides with the appropriate classification level.

15.2.3. The outer container will be marked with the address and return address only. The outer address of the package must not contain the recipient's name; however, you

may use their mail code or group designation (i.e., Attn: Technical Library, SCLBR-NM-T).

15.2.4. Both the inner and outer packages must be sealed with tamper-proof tape, lead seals, etc., in order to preclude tampering with in route.

15.3. Courier Procedures

15.3.1. The normal, preferred, method for transmission of classified material to another facility is through Federal Express. Occasionally, due to extreme urgency, classified material may be hand-carried to another cleared facility.

15.3.2. NMT personnel will not hand-carry material on trips that involve an overnight stop prior to reaching their destination.

15.3.3. The FSO must approve all courier authorizations. In order to do so, the FSO will:

- Verify the facility clearance and storage capabilities of the facility
- Brief the courier on his or her responsibilities for safeguarding the classified information
- Prepare a transmittal receipt for the classified material prior to departure and retain the third copy of the receipt in the Security Office
- Prepare a hand receipt showing the transfer of the material to the courier and from the courier to the recipient
- Package the material as though it were being mailed

15.3.4. The package must remain in the possession of the courier or be stored in a GSA-approved container at a cleared facility at all times.

15.3.5. If the courier brings the material back to EMRTC, an inventory of the classified material will be made. If the courier does not bring back the material, the receipt will be filed in the Security Office.

15.4. Receipts

15.4.1. A Transmittal receipt must accompany each classified shipment. The receipt will identify the classified contents, as well as the name and address of the sending and receiving facilities.

15.4.2. Receipts will not include classified information; a short title or abbreviation will be substituted (if necessary) for a classified title. A copy of the receipt will be retained in a suspense file until the signed copy is returned.

15.4.3. A 30-day suspense date will be established, and follow-up action will be initiated if the signed receipt is not returned within that 30 days.

15.4.4. If, after follow-up action has been taken, the signed receipt is still not returned, or the addressee indicates non-receipt of the material, an inquiry will be conducted in accordance with 32 CFR Part 117.15 (e)(2)(iii).

15.4.5. Copies of the signed receipts will be retained in the Security Office for a minimum of two years.

15.5. Release or Transmission outside the Facility

15.5.1. The FSO will obtain the contracting officer's written approval for the release of classified information outside this facility except in the following instances:

- When release is required in the specific terms of the contract;
- When it is necessary in the performance of the contract;
- In connection with pre-contract negotiations with prospective contracts, vendors, or suppliers;
- In prime contractor-subcontractor relationships; or
- During visits among prime contractors who are participating under U.S. Government direction in contracts pertaining to research, development, and production of a weapons system.

15.5.2. When a company not associated with a specific contract requests classified information generated or received under that contract, the written authorization of the contracting officer shall be sought before releasing the information.

16. REPRODUCTION OF CLASSIFIED MATERIAL NISPOM 117.15

- Prior to reproducing classified material, the FSO, or their designated representative, will be contacted for approval. Reproduction of classified information will follow the guidelines set for in 32 CFR 2001.45 (b).
- Copies of classified material will only be made when absolutely necessary, and to the minimum number possible.
- Classified material will only be reproduced on copy equipment that has been approved for classified reproduction. Rules governing the use of the designated equipment will be conspicuously posted on or near the equipment; appropriate warning notices prohibiting the reproduction of classified material will be posted on or near equipment not approved for classified reproduction.
- Classified reproductions will bear the same classification markings as the original document.
- Classified reproductions will be assigned an accountability control number.
- Incidents of classified reproduction will be noted in the "Reproduction Log", and the copies' disposition will be reflected in the master accountability record.

17. MARKING CLASSIFIED INFORMATION NISPOM 117.14

17.1. Classifying Procedures

17.1.1. The contracting officer will supply a DD Form 254, *Department of Defense Contract Security Classification Specification* to the individual creating the classified document.

17.1.2. The DD Form 254 specifies the level of classification required and provides classification guidance for specific information on what guide will be used for material related to that contract.

a. The Department of Energy (DOE) does not use the DD Form 254, but will supply guidance on the DOE Form F.5634.2, *Safeguards and Security Survey Report,* on request.

17.1.3. Whenever NMT originates potential classified information not in the performance of a contract or program, it will be protected as classified. The information will be treated as though it is classified at the appropriate level until a classification opinion is obtained from the UA with an interest in the subject matter.

17.1.4. The FSO will review the necessity, currency, and accuracy of all classified material generated at NMT.

17.2. Incorporating Classified Information into Other Documents

17.2.1. When a classified document or other material is jointed to, incorporated in, or otherwise made a part of another classified document or item of material, accountability for the original document or items will be terminated, and accountability for the document or items in which it was incorporated will be established.

17.3. Method of Generation

17.3.1. Computers and word processors will not be used for preparing classified information unless the system or equipment is approved in writing by DSS. The Associate Director of Safety, Security, and Environmental Compliance will approve all equipment and systems.

17.4. Working Papers

17.4.1. Classified working papers must be marked with the overall level of classification, the notation “Working Papers”, date of generation, printed and signed name of the originator, and contract number for supporting DD254. Classified working papers must be destroyed when no longer needed.

17.4.2. If working papers are retained for more than 180 days, and released outside of the facility, they must be marked in the same manner prescribed for a finished document at the same level.

17.4.3. Classified working papers will be stored in a GSA-approved container.

17.5. Accountability

17.5.1. NMT is required to account for all classified material. Classified material must be fully marked with the level of classification, who it was classified by, declassification information, NMT’s address, and date it is entered into accountability.

17.5.2. Material **Must** be entered into accountability when the first of any of the following events occur:

- The material is retained as a completed document in excess of 30 days from the date of generation,
- The material is reproduced,
- The material is retained as a partially completed document upon discontinuance of the work, or
- The material, regardless of its stage of development, is transmitted outside the facility.

17.6. Satellite Accountability Systems

17.6.1. There is only one control accountability system used at EMRTC.

17.7. Test Operations

17.7.1. Classified high-speed film, x-rays, still photos, etc. are considered completed materials at their time of generation and must be entered into accountability immediately. The following steps will be taken when generating classified material in the EMRTC Field Laboratory:

a. The Test Engineer/Manager will contact the FSO and request an accountability number which will be assigned to all classified material generated during that test's operations.

17.7.1.a.1. The numbers may be assigned on a daily basis, weekly, or series-long basis.

17.7.1.a.2. Classified tests will NOT be conducted without an assigned accountability number.

b. The Test Engineer/Manager will be supplied with security labels, and appropriate security classification guidance.

c. The Test Engineer/Manager will be responsible for insuring that each classified item (i.e., box of film, data sheet, yaw card, etc.) is properly marked with the accountability number, level of classification, declassification/classification instructions, NMT address, etc.

d. All classified material will be transferred to an approved secure storage area using an approved method of transfer.

e. The Test Engineer/Manager will notify the FSO of the classified material generated during each day of testing.

f. An inventory of the classified material generated under that number will be transferred into the master accountability log.

g. Working papers may still be generated, and are not required to be in accountability until they have existed 180 days from their date of initial generation. After 180 days, the material will be destroyed or entered into accountability.

18. MARKINGS NISPOM 117.14

Classified material will be marked in accordance with NISPOM 117.14

18.1. The FSO will ensure that all employees authorized to make derivative classification decisions will:

18.1.1. Be identified by name and position, or by personal identifier, on documents they derivatively classify.

18.1.2. Observe and respect original classification decisions.

18.1.3. Carry forward the pertinent classification markings to any newly created documents. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

a. The date or event for declassification that corresponds to the longest period of classification among the sources; and

b. A listing of the source materials.

18.1.4. Be trained at least once every two years, in accordance with CSA direction, in the proper application of the derivative classification principles, and with an emphasis on avoiding over-classification. Training will cover classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

18.1.5. Not be authorized to conduct derivative classification until they receive such training.

18.1.6. Be given ready access to the pertinent classification guides and/or guidance necessary to fulfill these important actions.

19. DISPOSITION OF CLASSIFIED MATERIAL

19.1. Quantity of Material

19.1.1. The quantity of classified material on hand will be minimized to the greatest extent possible, consistent with contractual performance.

19.1.2. Once classified information is no longer needed, it will be returned to the contracting officer or destroyed.

19.1.3. All classified materials must be associated with a specific contract. The contract must be active or authority obtained from the contracting officer as discussed in NISPOM 117.14 to retain a document or material after the contract has been completed

19.2. Destruction

19.2.1. Destruction may be accomplished by shredding, burning, pulping, melting, mutilation, chemical decomposition, or pulverizing. The FSO will determine which method is to be used depending upon the type(s) of material to be destroyed.

19.2.2. If materials are burned, the ash residue will be carefully inspected and reduced by physical disturbance to ensure no burned material survives intact.

19.2.3. Classified material in need of disposal shall be destroyed on the same day it has been removed from a cleared facility.

19.2.4. A Destruction Certificate will be completed for all classified material destroyed.

a. The Destruction Certificate will contain identification of the material, date of destruction, and will be signed.

b. Destruction records and certificates will be retained for a minimum of two years.

19.2.5. Classified material shall be destroyed by authorized personnel who have a full understanding of their responsibilities.

a. Two cleared witnesses are required for destruction of TOP SECRET and SECRET material.

b. Two cleared witnesses are required for the destruction of CONFIDENTIAL material.

19.2.6. Destruction of classified ordnance will be documented on the tests fire sheet(s). The Destruction Official will sign the test fire sheet certifying that the material in question has been completely destroyed.

19.2.7. Destruction of classified hardware/ordnance will be documented on a destruction certificate generated by the Security Office or on a hand-receipt form generated by the Test Engineer/Manager.

20. RETENTION OF CLASSIFIED MATERIAL NISPOM 117.14

20.1. Classified material will be returned, surrendered, or destroyed (if authorized) as follows:

20.1.1. Within 180 days after the opening date of bids, proposals, or quotes, only if a bid, proposal, or quote is not accepted.

20.1.2. Within 180 days after notification of non-acceptance if a bid, proposal, or quote is not accepted.

20.1.3. Within two years of a successful bid after final delivery of goods and services, or after completion or termination of the classified contract; whichever comes first. Further retention beyond the two-year period, must be requested and written retention authority receive from the GCA provided the GCA does not advise to the contrary.

20.1.4. Within one year after receipt if the classified material was not received under a specific contract, such as, material obtained at classified meetings or from a secondary distribution center.

21.CONTROL OF AREAS

Campus Police officers are responsible for reporting to the Chief of Campus Police for all violations of security measures.

21.1. Duties and Patrols

21.1.1. Provide a deterrent effect against possible security violations; the apprehension of such violators is of secondary importance. Officers will use their best judgment in apprehending trespass violators, force being used only as a last resort.

21.1.2. Officers will be especially alert at night, on weekends, and on holidays. Patrols will be spaced unevenly in time, and will be reserved in direction frequently.

a. Every effort will be made to avoid regular patrols that can be anticipated.

b. The EMRTC Security Office maintains a list of inspection stations. This list will be furnished to the Campus Police, and will be updated whenever necessary.

21.1.3. Written logs of each security patrol will be generated in each shift of each work day. Inspection of the records will be made to ensure patrols are being conducted correctly and effectively.

21.1.4. Campus Police personnel will review each written log for compliance with DSS requirements. Officers will be required to provide a written response for any checks within their shift that are more than 10 minutes late.

21.1.5. In order to ensure that required 4-hour check intervals are not exceeded between shifts, Patrol Officers will not make the last check at these facilities more than 1 hour before or after shift change.

21.1.6. If Patrol Officers are required to assist on campus, other officers in the field will make all necessary attempts to make the other officer's required checks. Officers will not remain on campus any longer than absolutely necessary before returning to their Field Laboratory checks.

21.2. Closed Area Patrols

21.2.1. Due to the unique nature and location of NMT's closed areas, Officers are not required to enter a closed area to verity if it is secure. The Officers only responsibility is to ensure the closed area is secure.

21.2.2. Additional perimeter control security will be provided by the Campus Police by random, unannounced inspections of personal belongings of personnel entering or exiting the Field Laboratory or the EMRTC Complex.

22. EMERGENCY PROCEDURES

22.1. Natural Disaster or Civil Disturbance Incapacitates Facility

22.1.1. In the event of a natural disaster or civil disturbance, which renders the facility incapable of safeguarding classified material, the FSO will submit a report to the Cognizant Security Office (CSO) as quickly as possible. Courses of action to be taken are:

22.1.2. Secure classified material in GSA-approved storage containers or controlled areas.

a. Examine GSA approved storage containers and controlled areas upon returning to the facility to determine whether the classified information has been compromised or if any classified material is missing.

b. If appropriate, a report will be submitted in accordance with the NISPOM.

22.1.3. Request assistance from appropriate civil authorities, including local and state law enforcement agencies.

- New Mexico State Police: 575-835-0741 or 575-835-0941
- Albuquerque FBI Office: 505-224-2000

22.2. Riot or Civil Disturbance on NMT Campus

22.2.1. In the event of a riot or a civil disturbance on the campus, the GSA-approved storage containers located on campus will be removed and secured within a closed area in the NMT Field Laboratory. Armed deputized, campus police will remain on guard at the facility until the disturbance ceases or until the classified material(s) have been removed.

22.3. Invoking Emergency Procedures

22.3.1. These emergency procedures will be invoked at the discretion of one or all of the following individuals:

- Director of EMRTC, 575-835-5701
- FSO, 575-418-7143
- Chief of Campus Police, 575-835-5555

23.REFERENCES

- 32 Code of Federal Regulations (CFR), Part 117 https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117

- Security Executive Agent Directive 3- SEAD 3 – Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf

23. ATTACHMENTS

1. Quick Reference Information
2. Defense Hotline Information
3. Required Data Elements for Reporting

ATTACHMENT 1

QUICK REFERENCE

NMT Commercial and Government Entity Number (CAGE) Code (or FSC Number): 4B850

New Mexico Institute of Mining and Technology was granted a Top SECRET Facility Security Clearance with TOP SECRET storage capability by Defense Industrial Security Clearance Office (DISCO) on March 15, 2001-

Classified Mailing Addresses:

NM Tech/EMRTC
Attention: Document Control
1001 South Road
Socorro, NM 87801-4796

Or

NM Tech/EMRTC
Attention: Document Control
P.O. Box 923
Socorro, NM 87801

NMT Cognizant Security Office:

Defense Security Service
Industrial Security Field Office
10851 N. Black Canyon Hwy (IOFWX)
Ste 860
Phoenix, AZ 85029

Facility Verification Data Base:

Industrial Securities Facilities Data Base

ATTACHMENT 2

DEFENSE HOTLINE

This hotline provides an avenue for DoD personnel and contractor employees to report, without fear of reprisal, known or suspected instances of serious security irregularities and infractions concerning defense affiliated contracts, programs or projects.

This facility will conspicuously post (e.g., common areas) information regarding the Defense Hotline and will inform all employees that the Defense Hotline may be used, if necessary, for reporting matters of national security interest.

The telephone number and address for the Defense Hotline is:

1-800-424-9098

Defense Hotline
The Pentagon
Washington, DC 20301-1900

ATTACHMENT 3

REQUIRED DATA ELEMENTS FOR REPORTING

When self-reporting or reporting about others is necessary, the following information must be provided in the report, as available and applicable.

1. Foreign travel:

    a. Complete itinerary.

    b. Dates of travel.

    c. Mode of transportation and identity of carriers.

    d. Passport data.

    e. Names and association (business, friend, relative, etc.) of foreign national traveling companions.

    f. Planned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (business, friend, relative, etc.).

    g. Unplanned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (post-travel reporting).

    h. Name, address, telephone number, and relationship of emergency point of contact.

    i. Unusual or suspicious occurrences during travel, including those of possible security or counterintelligence significance (post-travel reporting).

    j. Any foreign legal or customs incidents encountered (post-travel reporting).

2. Unofficial contact with a known or suspected foreign intelligence entity:

    a. Service(s) involved.

    b. Name of individual(s) contacted.

    c. Date(s) of contact.

    d. Nature of contact to include any unusual or suspicious activity.

    e. Likelihood of future contacts.

3. Continuing association with a known foreign national(s) or foreign national roommate(s):

    a. Name of foreign national(s).

b. Citizenship(s).

c. Occupation.

d. Nature of relationship, i.e., business or personal.

e. Duration and frequency of contact(s).

f. Current status of the relationship(s).

4. Involvement in foreign business:

a. Nature of involvement.

b. Countries involved.

c. Name of business.

5. Foreign Bank Account:

a. Financial institution.

b. Country.

6. Ownership of foreign property:

a. Location.

b. Estimated value.

c. Balance due.

d. Purpose and use of property.

e. How acquired.

7. Foreign citizenship:

a. Country.

b. Basis for citizenship.

c. Date of application or receipt.

8. Application for a foreign passport or identity card for travel:

a. Country.

b. Date of application.

c. Reason for application.

9. Possession of a foreign passport or identity card for travel:

a. Issuing country.

b. Number.

c. Date of issuance.

d. Expiration date.

e. Reason for possession.

10. Use of a foreign passport or identity card for travel:

a. Issuing country.

b. Reason for use.

c. Date(s) and country(ies) of use.

11. Voting in a foreign election:

a. Date.

b. Country.

c. Election.

12. Adoption of non-U.S. citizen children:

a. Country involved.

b. Foreign government organization involved.

c. Foreign travel required.

d. Adoption agency or other intermediary.

e. Adoptive parents' current linkage to foreign country.

13. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure:

a. Date(s) of incident.

b. Name of individual(s) involved.

c. Nature of incident.

d. Method of contact.

e. Electronic address.

f. Type of information being sought.

g. Background, circumstances, and current state of the matter.

14. Media contacts:

a. Date(s) of contact.

b. Name of media outlet.

c. Name of media representative.

d. Nature and purpose of contact.

e. Whether classified information or other information specifically prohibited by law from disclosure was involved in the contact.

f. Current status of the contact.

15. Arrests:

a. Date(s) of the incident(s).

b. Location(s) of the incident(s).

c. Charges and/or circumstances.

d. Disposition.

16. Financial Issues and Anomalies:

a. Type of issue or anomaly (bankruptcy, inheritance, etc.).

b. Dollar value.

c. Reason.

17. Cohabitant(s):

a. Name(s).

b. Citizenship(s).

c. Date of Birth.

d. Place of Birth.

e. Duration of contact(s).

18. Marriage:

a. Name of spouse.

b. Citizenship of spouse.

c. Date of Birth.

d. Place of Birth.

e. Date of marriage.

19. Alcohol- and drug-related treatment:

a. Reason.

b. Treatment provider, to include contact information.

c. Date(s) treatment provided.

Signature: Cris Clayton
Cris Clayton (Apr 13, 2026 16:17:23 MDT)

Email: cris.clayton@emrtc.nmt.edu

SOP 401 Industrial Security Standard Practice Procedure 031926F

Final Audit Report 2026-04-13

Created:	2026-04-13 (Mountain Daylight Time)
By:	Troylyn Zimmerly Armijo (troylyn.zimmerly@adobe.nmt.edu)
Status:	Signed
Transaction ID:	CBJCHBCAABAAeYbFAEJ81WrFIpmzIVF21nvQR9TzMqmG
Number of Documents:	1
Document page count:	47
Number of supporting files:	0
Supporting files page count:	0

"SOP 401 Industrial Security Standard Practice Procedure 0319 26F" History

Document created by Troylyn Zimmerly Armijo (troylyn.zimmerly@adobe.nmt.edu)
2026-04-13 - 1:22:28 PM MDT

Document emailed to cris.clayton@emrtc.nmt.edu for signature
2026-04-13 - 1:23:19 PM MDT

Email viewed by cris.clayton@emrtc.nmt.edu
2026-04-13 - 4:16:50 PM MDT

Agreement viewed by cris.clayton@emrtc.nmt.edu
2026-04-13 - 4:16:50 PM MDT

Signer cris.clayton@emrtc.nmt.edu entered name at signing as Cris Clayton
2026-04-13 - 4:17:21 PM MDT

Document e-signed by Cris Clayton (cris.clayton@emrtc.nmt.edu)
Signature Date: 2026-04-13 - 4:17:23 PM MDT - Time Source: server

Agreement completed.
2026-04-13 - 4:17:23 PM MDT