NEW MEXICO TECH
SCIENCE • ENGINEERING • RESEARCH UNIVERSITY

INITIAL/ANNUAL SECURITY BRIEFING

INTRODUCTION

The purpose of this briefing is to make you aware of the Department of Defense Security Program requirements and your responsibilities as a cleared employee.

The three levels of classification are listed below. Their unauthorized disclosure can cause the following to our Nation's Security:

- Top Secret – Grave Damage
- Secret – Serious Damage
- Confidential – Damage

A Security Clearance is an administrative determination for an individual who is eligible for access to classified information at a specific level. Only those individuals needed to meet contractual requirements shall be processed for a security clearance and requested by their immediate supervisor. If a cleared employee does not have access to classified material during a 12-month period; the access will be removed, and the employee will be debriefed, until the individual is tasked to support a classified contract again. The employee is considered one with "No Access." Upon needing access to classified material again the last investigation must be within the investigation scope; Top Secret requires a 5 - year scope and Secret requires a 10 - year scope. If the "No-Access" time frame has exceeded 24 months, the clearance is no longer valid and a re-application is required.
A de-briefing is required upon termination for all cleared employees.

"NEED TO KNOW"

"A person regardless of clearance or position should have access only to that information which is specifically required to accomplish his or her job duties."

Protection of classified information is directly tied to our National Defense and is based on clearance level and "Need-to-Know".

SAFEGUARDING

Classified material is always kept under constant surveillance. Cover or place face down to prevent unauthorized visual access. Store classified material in a GSA-approved container and limit the number of persons with combinations. The containers must be locked when not under the direct supervision of a cleared person.

A private written record of the container combination is not allowed. Removal of classified material to a private residence is prohibited and cannot be kept in an un-cleared facility such as a hotel room overnight.

Prior arrangements must be made for storage when hand carrying material on an overnight trip and prior to hand carrying any classified material. A special "Courier Briefing" is required.

ORIGINAL CLASSIFICATION

Only authorized government officials classify material. Private contractor employees do not have original classification authority. NM Tech employees approved to create derivative classification determinations are required to conform to the 32 CFR 2001.24(k)(4), NISPOM requires that contractor cleared personnel must be trained initially and at least once every 2 years on the topics set forth in NISPOM. Please see the Security Office for required training.

32 CFR 2001.24(k)(4).

Cleared contractor personnel who can document that they have completed initial derivative classifier training required by 32 CFR 2001.24(k)(4) NISPOM, do not need to take additional training until 2 years have elapsed from the date of their initial training.

- Contractors can develop and implement internal training programs or use an existing training course that includes, at a minimum, the topics set forth in 117.12 (h) to meet the NISPOM requirements of derivative classification training for contractor personnel who are authorized to make derivative classification decisions.
- Contractors will retain records of the date of the most recent training (initial or refresher) and type of training derivative classifiers receive. Records of training must be available for review during DCSA security vulnerability assessments. Records may consist of training attendance records, certificates, or other documentation verifying that personnel assigned duties as derivative classifiers have successfully completed the training requirements.

CLASSIFICATION GUIDANCE

Guidance from the government takes one or a combination of three forms:

- Guidance in marking may be derived from classified source material. When using classified source material, the author must carry over the classification of each portion from the source document to the next document.
- Guidance to contractors is provided by a DD254 which accompanies each classified contract providing classification guidance and classification instructions. In addition, the DD254 outlines any special requirements, access, levels or restrictions.
- Security Classification Guides – References made in the DD254 pertain to a particular military program and may apply to more than one contract. Each classification guide is categorized by topic, classification assigned that topic, downgrading or declassification instructions, and remarks that clarify the classification assignments for the author.

Classification cannot be reworded by restatement, sanitizing or unauthorized coding.

Employees are required to challenge any classification they have substantial reason to believe is inappropriate; whether it is over classified or under classified. Contact the Security Office if in question.

Until a classification decision is made, the information in question must be protected at the higher level of the existing or proposed classification.

Interior pages shall be marked top and bottom with the highest-level classification contained on it.

The highest level of classification shall be marked on each section, part or paragraph. Marking helps the user determine just what is classified and to what level.

Charts and photos shall be marked with the higher level of classification contained therein.

A title page must contain the overall classification, name and address of the facility/originator, date of the document was prepared, the "Classified By" or "Derived From" line and the "Declassify On" line.

The classification authority by which the document is classified must appear on the document. If multiple sources are used in classifying the document, the term, "Multiple Sources" may be used provided a bibliography of sources is maintained.

The most restrictive downgrading/declassifications must also appear on the document. The derivative classifier will carry forward either the instructions on the "Declassify On" line from the source document, or the duration instruction from the classification guide*. In 1995 Executive Order 12958 eliminated the use of "OADR" (Originating Agency Determination Required) on documents created after October 14, 1995.*

CLASSIFIED WORKING PAPERS

Classified working papers generated by the contractor in the preparation of a finished document shall be:

- Dated when created
- Printed and signed name of the originator
- Marked with its overall classification and with the annotation "Working Papers"
- Contract Number for supporting DD254 shall be listed on the "Working Papers"
- Destroyed when no longer needed
- Store in a GSA-approved container

Working papers shall be marked in the same manner prescribed for a finished document at the same classification level when:

- Transmitted outside the facility, or
- Documents retained for more than 30 days from creation for Top Secret, or 180 days from creation for Secret and Confidential material.

CLASSIFIED WASTE

Classified waste must be safeguarded in a GSA-approved storage container. Approval must be obtained from the Security Office before destruction of classified waste. Classified waste includes: Preliminary drafts, carbon sheets, plates, stencil masters, and worksheets.

REPRODUCTION

Secret and Confidential material may be reproduced to meet operational needs. Department of Defense will provide written authorization to the Security Office for printers used for classified reproduction.

All reproductions will be administered by the Security Office staff. Special reproduction requirements may apply to some classified information. Contact the Security Office for guidance.

Reproductions must be marked with the same classification as the original, placed into accountability and safeguarded.

Classified material being transferred within the facility shall have an appropriate cover sheet attached or be otherwise covered to prevent unauthorized visual access and accompanied with a transmittal receipt. The material being transmitted must remain under the direct supervision of the authorized cleared individual.

Classified material may not be transferred to any location or any employee until it has been established that the recipient has a need-to-know, the appropriate clearance level and approved storage facility.

An external transmission of classified material, either hand-carried or mailed, must be processed through the Security Office.

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CUI is an umbrella term that includes Unclassified Controlled Technical Information (UCTI), Sensitive but Unclassified (SBU), For Official Use Only (FOUO), and Law Enforcement Sensitive (LES). For information to be considered CUI it must fall within a category, such as:

- Critical Information
- Defense
- Export Control
- Financial & Tax
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural & Cultural Resources
- NATO
- Nuclear
- Patent
- Privacy
- Procurement & Acquisition
- Proprietary Business Information
- Provisional (for DHS use only)

- Statistical
- Transportation

A complete list of categories, sub-categories, and descriptions can be found at https://www.dodcui.mil/
All documents containing CUI are required to be marked (CUI Controlled, Controlled//Specified, etc.).
Marking guidance can be found at https://www.dodcui.mil/

CUI is similar to FOUI as it is handled, stored, transmitted, and destroyed in basically the same manner at the legacy FOUO program.

- When the option is available, should be processed on Government Furnished Equipment (GFE)
- Must be encrypted if sent via email
- Limit access to those with a lawful government purpose
- Destroyed by means approved for destroying classified or in a manner making it unreadable, indecipherable, and irrecoverable.
- After working hours, CUI will be stored in unlocked containers, desks, or cabinets if the government building provides security for continuous monitoring of access. If building security is not provided, the information will be stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas.
- CUI will be formally reviewed IAW DoDI 5230.09, Clearance of DoD Information for Public Release, before being decontrolled or released to the public.

CUI training can be accessed at https://securityawareness.usalearning.gov/cui/index.html

PUBLIC DISCLOSURE
NISPOM 32 CFR 117.15

Contractors will not disclose classified information to the public. Contractors will not disclose unclassified information pertaining to a classified contract to the public without prior review and clearance as specified in the Contract Security Classification Specification, or equivalent, for the contract or as otherwise specified by the GCA. The procedures of this paragraph also apply to information pertaining to classified contracts intended for use in unclassified brochures, promotional sales literature, reports to stockholders, or similar material.

CLASSIFIED VISITS
Visits made to other facilities requiring access to classified information must be coordinated through the Security Office in advance.

ADVERSE INFORMATION REPORTING REQUIREMENTS
Based on the guidelines set forth in the National Industrial Security Procedures Operating Manual 32 CFR part 117 aka "NISPOM Rule" cleared employees who are involved in unfavorable circumstances must report "Adverse Information" to the Department of Defense. Pursuant to this rule, Security Executive Agent Directive (SEAD) 3, available at https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf.

NM Tech requires that Adverse Information be reported immediately, but not later than the next duty day. 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. An inquiry will be conducted by the local security official or other designee to determine the cause and effect of the incident and the suitability of administrative or disciplinary action against the offender.

Adverse Information is 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 which could affect his or her ability to safeguard classified information. Examples of adverse information, which should be reported, includes: (Note: only factual information will be reported)

FOREIGN TRAVEL

- Report unofficial foreign travel in advance. Individuals must submit an itinerary and receive advance approval prior to travel. Unanticipated border crossings are discouraged.
- Be aware of any travel warnings or travel alerts for your destination country, which describe risks to you and may affect your travel plans.
- Any U.S. citizen traveling abroad on business or pleasure should be aware of the fact that they could be targeted by an intelligence agency.
- Follow up with the Security Office upon your return to determine if a post-briefing is required.
- Report any unusual incidents occurring during travel.

FOREIGN CONTACT

- A foreign national with whom one has a close and continuing contact. This individual may be a business/work associate, a boyfriend, girlfriend, relative's spouse, or family friend.
- Any attempt by a foreign national to solicit sensitive/classified information or other contact that you regard as suspicious.
- 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 to, investments in, or employment with foreign nationals and companies.

PERSONAL LIFE CHANGES

- Change of name
- Change in marital status (including legal separation)
- Change in cohabitation (involving a non-US citizen)

PSYCHOLOGICAL COUNSELING

- Consultation with a mental health professional (marital, family, and grief counseling need not be reported)
- Prescribed drugs as a result of psychological counseling

FINANCIAL CONCERNS

- Excessive indebtedness
- Liens
- Collections
- Bankruptcies
- Garnishments
- Judgments
- Identity theft
- Unexplained financial affluence over $10,000.00

COMPUTER/INFORMATION SYSTEM MISUSE

- Unauthorized access into an automated information system, whether government or contractor, for any reason
- Modification, destruction or manipulation of hardware or software on any government or contractor equipment

PASSWORD MISUSE

- Obtaining/using someone else's password
- Sharing a password
- Using a password to browse through another's account without permission
- Copying/Deleting information on another's account without permission
-

IMPROPER SECURITY PRACTICES

- Inadvertent or deliberate removal of classified information/materials to an unauthorized area
- Inadvertent or deliberate unauthorized destruction of classified information/materials
- Knowledge of a security violation or infraction and not reporting it
- Inoperability of locks, doors, vaults, etc., that are in place to secure classified information and/or materials
- Deliberate or inadvertent disclosure of classified information/materials to an unauthorized person
- Loss of classified information/materials
- Requests for classified or sensitive information/materials through unauthorized channels

ALCOHOL-RELATED ISSUES

- Arrests
- Treatment
- Counseling

DRUG USE

- Illegal/improper use of narcotics, non-medicinal drugs, non-prescription drugs, or controlled substances
- Previously unreported drug use
- Use of prescription drugs prescribed for someone else (friend, spouse, boyfriend, girlfriend, child, parent)

NOTE: The use of Cannabis is federal prohibited for cleared personnel

CRIMINAL CONDUCT

- All arrests (regardless of whether or not there is a conviction)
- Knowledge of a criminal act by another cleared individual

SECURITY VIOLATIONS

A Security Violation is any incident or situation, which could lead to the loss, possible loss, or compromise of classified information. Listed below are some examples of Security Violations:

- Classified material not secured properly in a GSA-approved container
- Processing classified information on an unaccredited Automated Information System (AIS)
- Classified Container left unlocked and unattended
- Discussion of classified on an unsecured telephone
- Unauthorized reproduction of classified information
- Unauthorized transmission of classified information
- Granting unauthorized personnel access to classified material
- Recording combinations – keeping them in a desk, wallet, etc.
- Combination locks not spun sufficiently. Spin them a minimum of 4 times in one direction

The person discovering the violation must safeguard the classified information involved when revealed and contact the Security Office immediately. The Security Office will conduct an administrative inquiry to establish the extent of the compromise, determine responsibility, initiate corrective actions, and prepare a report to the Defense Counterintelligence and Security Agency (DCSA) if required.

- First violation within a period of 12 consecutive months: Issuance of a security awareness letter, counseling by the FSO and supervisor, and any other corrective or disciplinary action deemed appropriate by an appointed committee. This committee shall be appointed by the employee's supervising Director
- 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
- 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.

SUSPICIOUS CONTACTS

Suspicious contacts include, but are not limited to, any efforts to gain illegal or unauthorized access to classified information or to compromise a cleared employee. In addition, all contacts by cleared contractor employees with known or suspected intelligence officers from any country, or any contact which suggests that an employee may be the target of an attempted exploitation by the intelligence services of another country shall be reported to your Facility Security Officer if actual, probable or possible espionage, sabotage, cyber intrusion attacks, terrorism or subversive activities at any of its locations.

REPORTING SUSPICIOUS ACTIVITY

Prompt and detailed reporting of suspicious activities can help prevent violent crimes or terrorist attacks. If you encounter suspicious activity, if you receive a suspicious email please report it to your Facility Security Officer or Physical Security Office as soon as possible.

Listed below are details to include in your report:

- Brief description of the activity
- Date, time and location of the activity
- Physical identifiers of anyone you observed
- Descriptions of individuals/vehicles
- Information about where people involved in suspicious activities may have gone
- Suspicious emails must contain headers

If in doubt, consult with the Security Office for a determination of reportable information.

CONTINUOUS EVALUATION

The Government has always relied on a system of self-reporting to ensure individuals still merit a security clearance. The requirement to self-report still remains although it is now enhanced with **continuous evaluation**.

According to the Director of Defense Counterintelligence and Security Agency, "Continuous evaluation allows us to monitor employees regularly throughout the tenure of their access to classified information. We regularly check about 22 different databases throughout the DoD, the U.S. government and the private sector to see if there are any indications that an individual is doing something that perhaps they shouldn't be doing. We hope to eventually reach the point where through the use of CE, we can eliminate the need to do secret-level reinvestigations and reduce the backlog of more than 700,000 cases."

All individuals will be placed in continuous evaluation. This means that the need to self-report adverse information is even more important.

The link below describes what you are required to self-report to your FSO and delineates the Adjudicative Guideline changes from 2005, and includes disqualifiers and mitigators. 2017 National Security Adjudicative Guidelines

INSIDER THREAT

DCSA defines the insider threat as: acts of commission or omission by an insider who intentionally or unintentionally compromises, or potentially compromises, the ability of an organization to accomplish its mission. These acts include, but are not limited to, espionage, unauthorized disclosure of information, and any other activity resulting in the loss or degradation of departmental resources or capabilities.

Every Cleared Defense Contractor (CDC) implemented an Insider Threat Program that requires you to report relevant information on *any* cleared person that is indicative of posing a risk to classified information and/or the CDC. You can make these reports to your FSO or the DoD Hotline at 800-424-9098.

HOW DO YOU RECOGNIZE AN INSIDER THREAT?

Potential Espionage Indicators:

- Suspicious emails must contain headers
- Failure to report foreign travel or contact with foreign nationals
- Seeking to gain higher clearance or expand access outside of the job scope
- Engaging in classified conversations without a need-to-know
- Working hours inconsistent with job assignment or insistence on working in private
- Exploitable behavior traits
- Repeated security violations
- Attempting to enter areas not granted access to

Not every person who exhibits one or more of these indicators is involved with illicit behavior, but most of the persons who have been involved with espionage were later found to have displayed one or more of these indicators.

REPORTABLE BEHAVIORS

Information Collection:

- Keeping classified materials in an unauthorized location
- Attempting to access sensitive information without authorization
- Obtaining access to sensitive information inconsistent with present duty requirements

Information Transmittal:

- Using an unclassified medium to transmit classified materials
- Discussing classified materials on a non-secure telephone
- Removing classified markings from documents

Additional Suspicious Behaviors:

- Repeated or unrequired work outside of normal duty hours
- Sudden reversal of financial situation or a sudden repayment of large debts or loans
- Attempting to conceal foreign travel

The link below delineates the Adjudicative Guidelines to include disqualifiers and mitigators: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-147

The above list of behaviors is a small set of examples. You should report any additional observed behaviors that may parallel or exceed the concerns listed in this briefing.

CONCLUSION

- Be Vigilant. Be Aware.
- If in doubt report – It is better to have reported overzealously than to never have reported at all.
- You are responsible for meeting all security requirements. It is an important responsibility and should not be taken lightly.

Should you have any questions regarding what you have just read, or any other security matters, please contact the Security Office.

Initial/Annual Security Briefing

I have read and will comply with the above Initial/Annual Security Briefing:

Print Name: _____

Signature: _____

Date: _____