UNM Annual Refresher Training For Cleared Personnel

INDUSTRIAL SECURITY
Publish or Perish

Academic Solicitation continues to be the top method of targeting and acquiring U.S. Technologies.

Protecting your research ensures that the work you have dedicated your life to is appropriately credited to you and not published or patented by other scientists or governments because your ideas or intellectual property were stolen either by a simple phishing email or while presenting at an international conference whether overseas or in the United States.

You may be working on something that has not yet been determined to be classified or export controlled information because it potentially has military application.

The Industrial Security Department is responsible for helping faculty, staff, and students with the security measures necessary to safeguard Classified, Sensitive, Intellectual Property, Export Controlled information, Controlled Unclassified Information (CUI) and Personal Identifiable Information (PII).

Contact 505-277-2058 for assistance
Foreign Interest Targeted Technologies

INFORMATION SYSTEMS

ARMAMENTS & ENERGETIC MATERIALS
Missile Systems, Warhead Technologies, Survivability Armor and Warhead Defeat Systems

SENSORS & LASERS

ALSO INCLUDED
Aeronautics
Space Systems
Marine Systems
Materials
Guidance/Navigation/Vehicle

ELECTRONICS
Microelectronics, Fabrication equipment, Electronic Materials, Components/Microwave Tubes, Microelectronics, Nanoelectronics
Annual Security Education Requirement

As cited in the National Industrial Security Program Operating Manual (NISPOM) 3-107, annual security training of employees engaged in classified work is required.

The contractor shall provide all cleared employees with some form of security education and training at least annually.

Refresher training shall reinforce the information that was provided during the initial security briefing and shall keep cleared employees informed of any appropriate changes in security regulations.

This training should be supplemented by work area training provided by your immediate supervisor or manager covering job specific security responsibilities.
Remember – Think OPSEC!

Do not make yourself a target, never advertise your clearance to anyone, including your friends, neighbors, or family.

80% of adversaries’ information is collected through open sources
- Blogs & Wikis
- Social networking sites (LinkedIn, Facebook, Twitter, Yammer)
- Foreign travel
- Conferences overseas or international conferences in the U.S.
Security Education Requirement & Access

Clearance + SF 312 + Need-to-Know = Access

Clearance:
Administrative action, usually involving a form
Classifications

Primary Classifications
Top Secret - Exceptionally Grave Damage
Secret - Serious Damage
Confidential - Identifiable Damage

Unauthorized disclosure could cause damage to the national security.

Other Classifications:
(Each of the following caveats require a supplemental briefing)
CNWDI
COMSEC
NATO
Restricted Data
Sensitive But Unclassified
NOFORN
FOR OFFICAL USE ONLY
Controlled Unclassified Information (CUI)
Classified Information or Material

Requires protection against unauthorized disclosure in the interests of national security.

Must always be under the control of an authorized individual.

Only be discussed or conveyed over approved communication devices such as secure telephones or sent via secure fax.

Only be stored in approved storage containers/areas.

Must be destroyed when no longer required.

Contact your Security Department for proper disposition instructions.

Must be properly marked regardless of the type of material (Documents, CD’s, Computers, Equipment, etc.)

Never be discussed in unauthorized areas or public places.

Never be left unattended.

Never be exchanged without first verifying personnel clearance and need-to-know.

Never be processed on your computer unless approved by the Designated Approval Authority.
Security Practices

Maintain physical protection in the work area
Always use classified information cover sheets
  Top Secret, Secret, & Confidential
Sanitize work area
Conduct end of day checks
Prevent disclosure of classified information to personnel
  without a security clearance
Always remember the need-to-know principle
Managers/Supervisors WILL provide employees with security
  training on responsibilities pertaining to their job duties.
Classification Guide
Markings, etc.
Approved Storage Containers

The University of New Mexico is authorized for classified storage and possesses a GSA approved container. It is important to know the following if access is granted:

- Government Classified material must be stored in GSA approved container.
- The combination must be protected at the same classification level as the material it is protecting. Therefore the combination is classified.
- Do not write down the combination anywhere.
- Do not verbally speak the combination out loud.
- Do not reveal the combination to anyone. If anyone asks for the combination, send them to the Security Department.
- When you are given the combination, you are accepting responsibility for safeguarding all of the classified information that it protects and stores.
- Daily open and close logs must be maintained.
Automated Information Systems (AIS)

The University of New Mexico does not have an AIS, but it is important to know the following:

Automated Information Systems used to capture, create, store, process, or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity, and to ensure the availability of the data and system.

Employees who receive an unauthorized and/or suspicious electronic transmission must immediately contact Security.
Do not erase or forward the transmission from your computer
Wait for direction from Security
What is Adverse Information?

Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that their ability to safeguard classified information may be impaired, or that their access to classified information may not be in the interest of national security.

Due to the sensitivity of adverse information it should only be reported to your site’s Facility Security Officer (FSO).
Reporting Requirements

Based on the guidelines set forth in the National Industrial Security Procedures Operating Manual (NISPOM) you should report the following to your FSO:

FOREIGN TRAVEL
Report all foreign trips in advance in which a pre-travel defensive security briefing is requested/required or if travel is to a HOT SPOT country. If you’re unsure is the country is a HOT SPOT then please contact your Security Officer.

• Business or personal travel (vacation, family emergency, etc.)
• Attendance at in international conference within the U.S.

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

• 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 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, grief counseling, and counseling need not be reported)
• Prescribed drugs as a result of psychological counseling

FINANCIAL CONCERNS
• Excessive indebtedness
• Liens/Collections
• Bankruptcies
• Garnishments
• Judgments
• Unexplained financial affluence of an accessed individual
Reporting Requirements (cont.)

**COMPUTER/INFORMATION SYSTEM MISUSE**
- Unauthorized entry 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 & not reporting it
- 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)

**CRIMINAL CONDUCT**
- All arrests (regardless of whether or not there is a conviction)
- Knowledge of a criminal act by another accessed individual
Suspicious Contact Reporting

Send suspicious emails with full headers and contact information of Foreign Nationals to FSO when you are requested to:

- Lecture overseas or in U.S. at an international conference
- Host a foreign national visit
- Review a CV for possible employment/study opportunity
- Relationship outreach
- Request for information
- Review a thesis or conduct peer research
- Ensure all sales and marketing requests are handled per company policy.
- Improper sales and marketing requests could easily circumvent export control policies and/or government regulations.
- Frequent international traveler, be wary of repeat accommodations. Collectors will place individuals in rooms that are “bugged” or otherwise under some type of surveillance.
Insider Threat Reporting

Previously, DOD required Cleared Defense Contractors (CDC’s) to protect the perimeter from outside security threats. Today, DSS requires all CDC’s to establish an Insider Threat Program that will gather, integrate, and report information indicative of a potential or actual insider threat. UNM’s plan was endorsed by the President of the University.

Each employee has a responsibility to ensure the protection of classified and controlled sensitive information entrusted to them. Be aware of potential issues and the actions of those around you and report suspicious behaviors to your FSO or the DOD Hotline (800-424-9098).

Reportable behaviors of others include but are not limited to:

- General disregard for security rules
- Failure to report overseas travel or contact with foreign nationals when required
- Use of alcohol or drugs
- Gambling
- Financial trouble
- Keeping classified materials in an unauthorized location
- Sudden reversal of financial situation
- Being disgruntled to the point of wanting to retaliate
- Making threats to the safety of people or property
What is a Security Violation?

Any failure to comply with established policy and procedures that reasonably could result in the loss or compromise of classified information.

Examples include:
- Disclosing classified information to any unauthorized person
- Leaving classified unattended (when at customer site)
- Failing to secure classified properly (when at customer site)
- Removing classified without authorization (from customer site)
- Discussing security procedures of closed areas to non-cleared personnel
- Failing to report a known or suspected compromise of classified information
- Deliberate disregard of security requirements
- Gross negligence in the handling of classified material (at UNM or when at customer site)
- A pattern of negligence or carelessness that was not deliberate in nature
Violations Not Reported

If violations are not reported:
- The correct mitigating actions are not taken.
- Damage assessments are not conducted.
- Compromised products continue to be developed and sold.
- Adversaries who obtain the compromised information can develop countermeasures.

When classified is compromised:
- Product effectiveness is reduced.
- Product use might actually help adversaries target personnel.
- This could potentially result in severe injury or death.
Examples of Unauthorized Disclosure

Title 18 U.S.C. Chapter 37  Espionage and Censorship

Examples

792. Harboring or concealing persons.
793. Gathering, transmitting or losing defense information.
794. Gathering or delivering defense information to aid foreign government.
795. Photographing and sketching defense installations.
796. Use of aircraft for photographing defense installations.
797. Publication and sale of photographs of defense installations.
798. Disclosure of classified information.
799. Violation of regulations of National Aeronautics and Space Administration.

Shall be fined under this title or imprisoned not more than ten years, or both for each charge.
UNM Foreign Visit Guidelines

Areas that are subject to Technology Control Plans (TCP) and areas faculty and security have deemed as sensitive are required to follow the below guidelines.

- Provide names of visitors for background check two (2) business days in advance to the FSO.
- Ensure there are a sufficient number of escorts to control the visit.
- Ensure escorts are briefed as to what is critical within the facility and that they know what requires protection from the foreign visitors.
- Ensure facility employees are briefed as to the scope of the foreign visit and to not discuss anything beyond what is approved.
- Be aware of “wanderers” who could discreetly place a USB in a computer.
- Do not permit any cameras or note taking if something in the facility is "sight sensitive."
- Secure visitor’s cell phones prior to the tour/visit.
- Do not allow suspicious unannounced foreign visitors access to the facility or space.
- Do not allow last minute additions or substitutions to a foreign delegation to have access to the facility or space.
- Foreign National Visitors are not authorized to use UNM computers, fax machines, copy machines, or similar equipment.

Contact your FSO if you need assistance during the visit
Cyber Security Reminders

Phishing emails are looking more real - IT blocks 1-3 million phishing/spam emails daily

- Do not click on links or attachments from suspicious looking emails
- Hover over links or return paths to determine real destination
- Look for a sense of urgency, spelling errors, poor grammar, warning that you have been a victim of fraud
- Use same precautions on your mobile device as you would on your computer

Rule of thumb: Anytime you are asked for personal information or your password – it is a scam
Hotlines

National Industry Security Program Operating Manual 1-207

Federal agencies maintain hotlines for government and contractor employees to report known or suspected instances of serious security irregularities and infractions concerning contracts, programs or projects.

- Department of Defense 1-800-424-9098
- Nuclear Regulatory Commission 1-800-233-3497
- Central Intelligence Agency 1-703-874-2600
- Department of Energy 1-800-541-1625

Contractor personnel are encouraged to furnish information through established company channels

Questions, comments, or concerns
Please contact your Facility Security Officer, Deb Kuidis, at 505-277-2058
Questions? Contact FSO at 7-2058