COMPREHENSIVE

Security Briefing

SEC 150

FOR

EMPLOYEES, CONTRACTORS,

AND CONSULTANTS

March 2007

Sandia National Laboratories

SAND2007-1758

SEC 150—Comprehensive Security Briefing

Table of Contents

Sandia is continually revising Corporate Process Requirements (CPRs) to capture the latest changes to Department of Energy (DOE) directives, federal and state laws, and Sandia's best management practices.

In the event of a discrepancy between a CPR and this briefing, the CPR takes precedence.

INTRODUCTION

Who Must Take SEC150?

You are receiving this briefing because:

- You have been granted a security clearance,
- Your clearance has been reinstated, or
- Your clearance has been transferred or extended from another facility.

The Purpose of this Booklet

This booklet discusses the important role you play in protecting national security, and you should familiarize yourself with its contents.

Classified Information Nondisclosure Agreement

Your security clearance fulfills the first of the three requirements that permit you to have access to classified information. The second requirement is to **sign** Standard Form 312 (SF 312), "Classified Information Nondisclosure Agreement," on page 42.

The purpose of SF 312 is to inform you of:

- The trust that is placed in you by providing you with access to classified information.
- Your responsibilities to protect that information from unauthorized disclosure.
- The consequences that may result from your failure to meet those responsibilities.

SF 312 is a contractual agreement between the United States Government and you, in which you agree never to disclose classified information to an unauthorized person. Upon completing your comprehensive briefing, you should:

1. Read SF 312.
2. Sign SF 312 in the presence of an authorized witness.
3. Hand the signed form to the authorized witness.

Need to Know (NTK)

The third requirement for accessing classified information is your need to know (NTK). That is, you must require access to classified matter to perform your official duties. As the holder of a security clearance, you are personally responsible for all classified matter and unclassified controlled matter (UCI or sensitive matter) that is entrusted to you. If you originate or use classified matter, you are responsible for determining a requester's identity, clearance, and NTK. Uncleared Members of the Workforce are allowed to access UCI as long as they have NTK.

Sandia's Security Objectives

The DOE and Sandia have four major security objectives that you should assume as your own:

1. Protection of Special Nuclear Material (SNM)

As a Class "A" facility, Sandia National Laboratories (SNL) could have SNM in its inventory at any time. The control and protection of SNM is critical, because of its potentially damaging effects should it fall into unauthorized hands.

2. Protection of Classified Matter

All Members of the Workforce are responsible for preventing the compromise, unauthorized disclosure, or loss of classified matter. You should:

- Be able to identify unattended classified matter.
- Know the appropriate reporting requirements (see pages 19-20).
- Before allowing access to such matter, establish the requestor's identity (examine the person's badge), proper clearance level, and NTK.

3. Protection of Unclassified Controlled Information (UCI)

UCI is sensitive matter that can help unauthorized sources gain valuable information to threaten our national security. Be alert! Protect all sensitive information from unauthorized sources.

4. Protection of Government Property

All property at SNL is owned by DOE and supported by taxpayers. Equipment and resources entrusted to you in your work must be given due care and accountability.

Security Education and Awareness Responsibilities

Manager's Responsibilities

Sandia managers are responsible for:

- Encouraging good security habits in all Members of the Workforce, including employees, contractors, and consultants.
- Promoting the proper protection of classified matter, UCI, government property, and Sandia assets.
- Integrating security awareness, controls, and requirements into all activities.
- Ensuring that Members of the Workforce receive appropriate training prior to working with classified matter and special nuclear material (SNM).
- Advising team members of any work-area-specific security practices.

All Members of the Workforce should:

- Be aware of any specific requirements that apply to their job functions, facilities, or work areas.
- Receive security training commensurate with their security responsibilities beyond this briefing. For example, you will require training if your job responsibilities include working with classified matter, UCI, or SNM.

Required Security Briefings

SNL's Education and Awareness Program provides four briefings as required by DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

Initial Security Briefing *(SEC050)*

The Initial Security Briefing provides basic information about SNL, its Safeguards & Security program, and related policies. The Initial Security Briefing (SEC050) is for all uncleared Members of the Workforce before they receive a DOE standard security badge and before they are given unescorted access.

Comprehensive Security Briefing *(SEC150)*

The Comprehensive Security Briefing (SEC150) must be received upon the granting of clearance and before receiving initial access to classified matter or SNM. This briefing provides:

- In-depth information on Sandia's security operations and requirements.
- Information on individual security responsibilities.

Annual Security Refresher Briefing *(SEC100)*

Members of the Workforce who hold a DOE clearance must complete the Annual Security Refresher Briefing (SEC100) within 12 months of the Comprehensive Security Briefing (SEC150), and every 12 months thereafter, for as long as they maintain their security clearance. This briefing may be completed online or by hardcopy.

- Coordinating this briefing for **contractors** is a shared responsibility between the line manager and employer.
- Coordinating this briefing for **consultants** is the sole responsibility of the line manager.

Termination Briefing *(SEC225)*

The Termination Briefing (SEC225) emphasizes your continuing responsibility not to disclose classified matter to which you have had access while at SNL.

The Termination Briefing also discusses your obligation to return all classified and UCI documents in your possession, and the potential penalties for noncompliance.

This briefing is held:

- When you take a leave of absence for 90 or more working days.
- On the last day of your employment.
- On the last day you possess an access authorization.
- On the day it becomes known that you no longer require access to classified information or SNM.

SECURITY AREAS

Security areas contain Safeguards & Security (S&S) interests that require physical protection.

Types of Security Areas

The types of security areas used within DOE and SNL include property protection areas, Limited areas, Exclusion areas, Protected areas, Material Access areas, and Vital areas, as well as more specialized security areas.

- **Property protection area (PPA):** Has defined boundaries established for the protection of DOE property.
- **Limited area (LA):** Protects classified information and has boundaries identified by barriers.
- **Exclusion area (EA):** Protects classified information and requires additional NTK authorization. Members of the Workforce usually are required to obtain permission before entering.
- **Protected area (PA):** Protects Category II quantities of SNM and classified matter. Defined by fences and walls, and surrounded by intrusion detection and assessment systems.
- **Material access area (MAA):** Protects Category I quantities of SNM.
- **Vital area:** Located within a Protected area and has separate perimeter and access controls to afford layered protection, including intrusion detection for vital equipment.

Note: While entering or within any security area:

- Check for posted signs in the areas being accessed.
- If visitors are present, verify the level of clearance required to enter the area.

Search Policy

Upon entering or leaving Sandia-controlled premises, all Members of the Workforce may be subject to a search of their persons, vehicles, and other belongings. In particular, a Security Police Officer may ask to examine all containers (e.g., packages, boxes, briefcases, handbags) to ensure that:

- No contraband is introduced.
- No government property or classified matter is taken without authorization.

Prohibited Items

Items prohibited on all Sandia-controlled premises without prior authorization include:

- Firearms.
- Explosives, pyrotechnics, propellants.
- Illegal drugs and paraphernalia, intoxicants.
- Any other items prohibited by law.

If you need to enter a corporate access-controlled building, contact the building manager and a) ask to be added to the access list b) verify the proper exiting procedures for times when you must work after hours.

If you're in a building and can't find the exit, look for a turnstile or locate a phone and call for assistance.

There are additional policies for Limited and more restricted areas. The following personally-owned items are prohibited without prior authorization:

- Radio frequency-transmitting equipment.
- Recording equipment (e.g., audio, video, data, etc.).
- Computers, peripherals, and associated media.
- Cell phones.
- Portable electronics (including hand-held computing devices).

For additional requirements and information, see CPR400.2.10, *Using Information Technology (IT) Resources,* Section 4.8, "Prohibited and Controlled Electronic Devices and Media"; CPR400.3.11, *Access Controls* and CPR400.3.16, *Cellular Phones*.

Vehicle Access

Personal vehicles are not permitted in LAs. Exceptions of up to 180 days (e.g., for health reasons) may be approved by Sandia Medical, per CPR300.5.7, *Medical Restrictions*.

Government and company vehicles (e.g., from sub-contractors) are always subject to search upon entering and exiting LAs. Additionally, both sides of a company vehicle must display the logo of the company with which the vehicle is affiliated.

Access to Security Areas After Hours

After normal working hours most buildings at SNL are locked and alarmed. Many buildings have an access-control system as indicated by a badge reader and/or keypad. Some buildings are controlled 24 hours per day and some are controlled only after working hours.

For example, some access-controlled buildings are configured in such a way that you do not have to call Security before leaving the building after hours. Some buildings, however, do require that you notify the Protective Force first (see contact lists on pages 34-39).

COUNTERINTELLIGENCE

Sandia's Counterintelligence Mission

The Office of Counterintelligence's mission is to detect, deter, and mitigate foreign intelligence collection and espionage efforts and international terrorists' threats against National Nuclear Security Administration (NNSA) personnel, classified and other sensitive programs, and information architecture.

The Counterintelligence Program protects DOE and SNL interests with awareness/education, briefings, debriefings (data collection), intelligence community liaison/investigative assistance, and data analysis. These integrated, centralized efforts target foreign and domestic intelligence and economic espionage threats.

Counterintelligence Reporting Requirements

Notify the Office of Counterintelligence if you:

- Have a substantive interaction with a sensitive country foreign national. Substantive interactions include:
  - Personal contacts that involve sharing private information and/or the formation of emotional bonds.
  - Professional conversations that generate discomfort because of the sensitivity of the subject being discussed.
  - Business or financial interactions with foreign nationals from sensitive countries.
- Are approached or contacted by any unauthorized person requesting classified/sensitive information.
- Suspect you have been approached by a foreign intelligence service (FIS), become an FIS target, or if you have knowledge or information of FIS targeting or recruitment attempts.
- Receive unsolicited e-mail directed to you from a sensitive country foreign national.
- Are approached by anyone (including a Member of the Workforce) who is seeking information for which they do not have NTK.

- Are uncomfortable about a fellow Member of the Workforce who:
  - Appears to be living well beyond their means.
  - Has unusual foreign contacts or travel.

How Adversaries Collect Intelligence

- **Human Intelligence:** Derived from or collected by human resources.
- **Open Source Intelligence:** Gathered from public sources, such as the internet, environmental impact statements, TV, and radio.
- **Imagery Intelligence:** Captured from sources ranging from satellites to hand-held cameras.
- **Signals Intelligence:** Emitted from voice, video, Morse code, and fax communications.
- **Measurements and Signature Intelligence (MASINT):** Quantitative and qualitative analysis of data from technical sensors.

OPSEC

OPSEC Legislation

In 1988, President Ronald Reagan issued National Security Decision Directive 298 (NSDD 298), which established a national Operations Security (OPSEC) program. This directive mandates a formal OPSEC program for each executive department and agency that is assigned to or supports national security missions with classified or sensitive activities. The directive describes OPSEC as:

> A systematic and proven process by which the U.S. government and its supporting contractors can deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive government activities.

DOE complies with NSDD 298 directive through DOE M 470.4-4, *Information Security*, Section B, "Operations Security."

Sandia's OPSEC Program

Adversaries thrive on collecting as much data as they can pull together—like combining puzzle pieces—to get the "big picture" about critical projects and resources. Thus, Sandia's OPSEC applies to all classified and sensitive activities conducted at SNL. It focuses on equipping Members of the Workforce with procedures and measures to protect programs and staff. All OPSEC activities are based on five steps:

1. Identify critical information
2. Analyze threats
3. Analyze vulnerabilities
4. Assess risk
5. Apply appropriate countermeasures

In addition, OPSEC reviews are performed in each organization that handles sensitive information at a frequency designated by Section B of DOE O 470.4-4, *Operations Security*. These reviews help to determine the level of OPSEC support required by a program or facility. They focus on *fact finding*, not fault finding, and will provide organizations with the details needed to make informed decisions regarding future OPSEC support.

Practice OPSEC Every Day

A strong OPSEC foundation is built on:

- **Building good habits:** Small steps taken daily to protect your information lead to a life-long habit of practicing good OPSEC.
- **Team effort:** An OPSEC program is only as strong as its weakest player. An *informed, aware* person is the most important part of an OPSEC program.

Practice OPSEC when:

- Using non-secure telephones and fax machines.

- Working with computers and e-mail communications.
- Holding casual conversations at work or off-site after hours.
- Disposing of trash or recycled paper.
- Conducting routine business activities.

Forms and requirements on interacting with FNs is available on the Foreign Interactions Office homepage. Search "Foreign Interactions" on the Tech Web.

FOREIGN INTERACTIONS AND FOREIGN TRAVEL

Foreign Interactions

Foreign National Access

Members of the Workforce who provide foreign nationals (FNs) with access to unclassified information, technologies, programs, and Sandia-controlled premises must first submit a Foreign National Request (FNR) Security Plan for approval. The FNR Security Plan must specify:

- Individuals who are approved to host, co-host, and/or escort the FN.
- Approved buildings and rooms.
- Approved access dates.
- Approved scope of work.

FNs may be vouched into a Limited area (LA) only by an authorized host, co-host, or escort listed on the approved FNR Security Plan, and only when the approved area is listed on the FNR Security Plan. Uncleared FNs wear site-specific badges with a red background.

Forms and requirements on foreign travel are available on the Foreign Interactions Office homepage. Search "Foreign Travel" on the Tech Web.

Foreign Travel

Requesting Business Travel

DOE requires Members of the Workforce to obtain approval for all official foreign travel prior to departure. This includes travel that is sensitive, non-sensitive, DOE-funded, Work for Others (reimbursable), and funded by indirect monies. There are many restrictions on the equipment you may take on foreign travel, and a long lead time is necessary when planning trips.

The deadlines for submitting business-related foreign travel trip requests to the Foreign Travel Office are:

- Non-sensitive official foreign travel – 37 calendar days prior to departure date.
- Sensitive official foreign travel – 52 calendar days prior to departure date.

For details and requirements consult the Foreign Travel help line (845-1300).

Reporting Personal Travel

All employees, contractors, and consultants (regardless of whether they hold a DOE clearance) must report **all** foreign travel to sensitive countries through the corporate Travel Information System prior to departure or as soon as is practical.

Exercise caution in dealing with citizens of any country to ensure that sensitive information, although unclassified in nature, is not inadvertently disclosed. This includes information about nuclear and other U.S. technology and the economy.

Travel to non-sensitive countries should be documented by Members of the Workforce, for future reference during clearance reinvestigations.

CLASSIFYING INFORMATION

About Classification

Classification is the identification of information that needs to be protected in the interest of national security. Through classification, Sandia safeguards important information from adversaries, yet allows its use by individuals who have the appropriate access authorization (clearance) and NTK.

DOE policy requires that classification decisions be made by Derivative Classifiers (DCs) who are knowledgeable in their technical fields and properly trained in classification.

Unclassified Controlled Nuclear Information (UCNI) Reviewing Officials (ROs) are the only persons authorized to determine that a document is UCNI. Many DCs are also UCNI ROs.

Your Classification Responsibilities

You must comply with the DOE policy of NTK and consult a DC to make a derivative classification determination. However, as a Member of the Workforce you are required to protect information/material that you suspect might be classified even before getting a DC classification determination.

Any services that your DC cannot provide should be handled by the Classification Department (see contact lists on pages 34-39). If you think that your DC's determination is inaccurate, you may appeal the ruling all the way up the chain to DOE Headquarters. The Classification Office can assist you with this process. DOE policy guards against retribution for an appeal to a classification decision.

If classified information is inadvertently compromised and you are approached for further information, DOE policy mandates that you respond "No Comment." You may refer inquiries to Media Relations (see contact list on pages 34-39).

Categories of Classified Matter

There are three categories of classified matter: Restricted Data (RD), Formerly Restricted Data (FRD), and National Security Information (NSI).

Restricted Data (RD):

- Is the most restrictive of the three classification categories.
- Consists of atomic energy information authorized for classification under the Atomic Energy Act and remains classified unless officially declassified by DOE.
- Includes all data about the design, manufacture, or use of atomic weapons, production of SNM, and the use of SNM in producing energy. Examples include: Inertial confinement fusion, nuclear directed energy systems, isotope separation, naval reactors.
- Does **not** include data declassified or removed from the RD category.

Formerly Restricted Data (FRD):

- Is classified information jointly identified as such by DOE and the Department of Defense, primarily related to the military use of atomic weapons.
- Is RD that has been transferred to the lower FRD category but remains classified, often referred to as transclassified.
- Must be handled as RD when transmitted to foreign countries.
- Includes information on weapon yields, location, safety, and storage; stockpile quantities; and other information the military needs to carry out its nuclear weapon responsibilities.

National Security Information (NSI):

- Requires protection (as determined by executive order) from unauthorized disclosure in the interest of national security.
- Information that does not pertain to nuclear systems, but has been determined per Executive Order 12958 (and any predecessor orders) to require protection against unauthorized disclosure. Examples include: Information about safeguards and security, weapon carriers, and missile and satellite technology.

Levels of Classified Matter

Each category of classified mater is subdivided into three levels: Top Secret (TS), Secret (S), and Confidential (C). The level indicates the degree of potential damage to national security if the matter were compromised.

- **Top Secret (TS):** Unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security.
- **Secret (S):** Unauthorized disclosure could reasonably be expected to cause serious damage to national security.
- **Confidential (C):** Unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security in the case of RD/FRD, or damage national security in the case of NSI.

Categories / Levels	Restricted Data	Formerly Restricted Data	National Security Information
Top Secret	TSRD	TSFRD	TSNSI
Secret	SRD	SFRD	SNSI
Confidential	CRD	CFRD	CNSI

General Guidelines

- **Only one classification for an entire classified work can exist.** Although the individual "parts" of a document or material may have different classifications. For example, a document may contain SRD and CNSI. The highest (most restrictive) category and level of any part of the work determine the classification for the entire work. In this example, the document must be classified as SRD.
- **RD and FRD** do not normally require portion marking.

- **NSI documents** are required to be portion marked.

Unclassified Controlled Information (UCI)

DOE and other federal agencies require access controls on certain scientific and technical information, even though that information is not classified. This type of sensitive information is referred to as UCI. As with classified information, access to UCI is limited to those with NTK for the performance of their official or contractual duties and who have had the required training. Types of UCI include by are not limited to:

- **Official Use Only (OUO)**: The most common type of UCI at SNL.
- **Unclassified Controlled Nuclear Information (UCNI):** Must be reviewed by an UCNI RO. The Classification website (see contact list on pages 34-39) can help you locate a UCNI RO and provide more information on UCNI requirements.
- **Naval Nuclear Propulsion Information (NNPI):** All information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance and repair of the propulsion plants of Naval nuclear-powered ships and prototypes. It is controlled in accordance with NAVSEAINST C5511.32B, and may require markings beyond OUO.

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

Controlling Classified Matter

- If you own classified matter, you are responsible for safeguarding access to it.
- Ensure individuals have the proper clearance level and NTK before permitting them to have access to classified matter.
- Control classified matter against unauthorized access at all times.
- Manage classified matter in an established Classified Work Station (CWS).
- Work with the assigned Classified Administrative Specialist (CAS) to control classified matter.
- Immediately report incidents involving lost or unaccounted for classified matter to your manager. If your manager is not available, report the incident to another manager or call OOPS (311).

Creating Classified Matter

- If you originate classified matter, you must apply proper markings and coordinate classification reviews.
- Work with your CAS to review markings and to mark classified matter.
- Ensure all classified documents have appropriate cover sheets.

Using Classified Matter

- Use classified information within line of sight and under your personal attendance.
- Classified matter must be covered with an appropriate cover sheet.
- You may relinquish control of classified matter only to those who have the appropriate clearance and NTK.
- Coordinate with your CAS on all reproduction of classified matter.
  - Only the minimum number of copies for operational necessity may be reproduced.
  - Only approved copiers can be used to reproduce classified matter.

Storing Classified Matter

- Protect classified matter by securing it in an approved repository when not in use.
- Approved repositories are GSA-approved safes, approved vaults, and VTRs.
- Ensure the appropriate CAS knows where classified is stored.

Technical Security Systems (TSS) installs, designs, and maintains building alarms, vault, and VTR alarms as well as badge readers.

For additional information, consult TSS (see contact lists on pages 34-39).

Moving Classified Matter

- Always work with your CAS.
- Mail, ship, or hand-carry classified matter only to authorized recipients and those with NTK.
  - Use Sandia mail and shipping services to mail and ship classified matter.
  - Internal recipients must have an approved CWS.
  - External recipients must have a DOE-approved Classified Matter Mail/Shipping Channel.
- If you originate classified information with access control markings, you must ensure that the intended recipient has the appropriate access authorization and NTK.
- Hand-carry classified matter as a last resort and only if you have:
  - An active, DOE-approved mail channel at the destination.
  - A current Annual Hand-Carry Briefing (SF 2902-AHB) on file.
  - A copy of the handcarry log.
- When transporting classified documents within Kirtland Airforce Base but outside of SNL, or off of Kirtland Airforce Base, you must ensure the documents are double wrapped or a Sandia-authorized double hand-carry bag is used.
- Receipts for classified matter must be created and signed, per CPR400.3.12, *Management of Classified Matter*. At SNL/CA, please see the *Classified Procedures Manual*.

Destroying Classified Information

- Always coordinate destruction with the appropriate CAS.
- Destroy classified matter in accordance with the Sandia Records Retention and Disposition Schedule.
- Use approved destruction methods to ensure classified matter is physically altered, demolished, or reduced to a useless form in such a way that no classified information can be obtained from it, or send it to the Waste Destruction Site in a red destruct bag.

Questions regarding Classified Matter Channels should be directed to the CMPC Coordinator (see contact lists on pages 34-39.

Classified Removable Electronic Media (CREM) and Accountable Classified Removable Electronic Media (ACREM)

CREM

Classified Removable Electronic Media (CREM) are those materials and components used for the purpose of providing non-volatile storage of classified digital data capable of being read by a computer. "Removable" refers to media that:

- Are designed to be introduced to and removed from the computer without adverse effect on computer functions.
- Can be separated from the computer.
- Include portable, electronic devices, such as laptop computers with fixed internal hard drives.

ACREM

CREM becomes accountable when it stores one of the following types of information:

- Top Secret (TS)
- Secret Restricted Data (SRD)
- Sigma 14 and Sigma 15

ACREM may also be removable electronic media that are accountable because they contain information on national, international, or programmatic requirements that address:

- Any electronic media with write capability, when introduced to an SRD or higher system.
- Deployable classified computer equipment and media supporting a nuclear emergency.
- Cryptography and designated Communications Security (COMSEC).
- NATO ATOMAL ("ATOMAL" is a NATO term used to indicate a special category information marking for designated "Restricted Data" or "Formerly Restricted Data" that is classified by the Atomic Energy Act of 1954).
- Designated United Kingdom (UK) information.
- Foreign government information designated in international agreements.
- Special access programs.

Your ACREM Responsibilities

Members of the Workforce who handle ACREM must:

- Work with their CAS to control ACREM and enter it into a formal, approved accountability system.

- Know the requirements for managing ACREM.
- Accept responsibility for all ACREM that they check out, per CPR400.3.12.3, *Management of Accountable Classified Documents at SNL/NM and Remote Sites,* Attachment D, "Accountable Classified Removable Electronic Media (ACREM)." At SNL/CA, please see the *Classified Procedures Manual*.
- Ensure that ACREM within their control, regardless of form, are afforded a level of protection against loss or compromise commensurate with their classification level(s).
- Not lend ACREM to others after they have checked it out.
- Ensure that classification levels and categories of ACREM are appropriate for the computer system accreditation level used to process the data.

Additional information and requirements on ACREM can be found in CPR400.3.12.3, *Management of Accountable Classified Documents at SNL/NM and Remote Sites*, Attachment D, "Accountable Classified Removable Electronic Media."

At SNL/CA, please see the *Classified Procedures Manual*.

MATERIAL CONTROL AND ACCOUNTABILITY (MC&A)

Sandia must maintain an effective MC&A program to possess and use accountable nuclear material. Management of accountable nuclear material helps ensure that it is properly characterized, controlled, protected, used, and accounted for, thereby detecting and deterring theft, diversion, or unauthorized use.

Sandia's MC&A program accomplishes this by generating and maintaining accurate information regarding nuclear material quantity, location, and other characteristics, and reports information to DOE's national nuclear material database.

Types of Accountable Nuclear Material

Accountable nuclear material is divided into three types:

- SNM
- Source Nuclear Material
- Other Nuclear Material

All accountable quantities of nuclear material must be stored in a Material Balance Area (MBA) and controlled, inventoried, measured, and tracked through an accountability (database) system.

Special Considerations for SNM

SNM is fissionable nuclear material (such as enriched uranium or plutonium) that releases energy when its atoms are split. Because of this capability, SNM is used for nuclear weapons. SNM therefore must be guarded to prevent possible theft or sabotage. The amount of SNM is characterized by "category." Category I is the highest quantity and Category IV is the lowest quantity group. A Category I or II quantity of nuclear material requires a higher level of physical security protection that includes protection within a Material Access area (MAA).

REPORTING REQUIREMENTS

General Reporting Requirements

Executive Order 12968, *Access to Classified Information,* makes a very serious demand on all Members of the Workforce. It states:

> Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.

Maintaining your security clearance is essential to your job. To maintain your security clearance, you must follow all reporting requirements.

IF YOU	YOU MUST REPORT THIS	TO
Are arrested, have criminal charges brought against you (including charges that are dismissed), or are detained by federal, state, or other law enforcement authorities for violations of the law, within or outside of the U.S. **Note:** Traffic violations for which a fine of $250 or less was imposed do not have to be reported unless the traffic violation is alcohol or drug related.	Orally, within 2 working days of occurrence. In writing, within the following 3 working days.	Corporate Investigators
File for bankruptcy, regardless of whether it is for personal or business-related reasons.	Orally, within 2 working days of occurrence. In writing, within the following 3 working days.	Corporate Investigators
Have your wages garnisheed for any reason. Examples: divorce, debts, child support.	Orally, within 2 working days of occurrence. In writing, within the following 3 working days.	Corporate Investigators
Are a current U.S. citizen who changes citizenship or establishes dual citizenship. Are a foreign citizen who changes citizenship. Change your name.	Orally, within 2 working days of occurrence. In writing, within the following 3 working days.	Personnel Security Foreign Interactions Office
Marry or cohabitate in a spouse-like relationship.	In writing (DOE Form 5631.34, *Data Report on Spouse/Cohabitant* within 45 working days of marriage or cohabitation.	Personnel Security

IF YOU	YOU MUST REPORT THIS	TO
Are approached or contacted by any individual seeking unauthorized access to classified information or matter, or SNM.	Orally, within 2 working days of occurrence. In writing, within the following 3 working days.	Counterintelligence, Corporate Investigators, or SIMP Pager
Are hospitalized for a mental illness or for treatment of alcohol or drug abuse.	Orally, within 2 working days of occurrence. In writing, within the following 3 working days.	Corporate Investigators
Are employed by, represent, or have any other business-related association with a foreign or foreign-owned interest, or foreign national.	Orally, within 2 working days of occurrence. In writing, within the following 3 working days.	Foreign Interactions
Have business-related foreign travel to sensitive countries. Have business-related foreign travel to non-sensitive countries. Have personal foreign travel to sensitive countries. Note: You are not required to report personal foreign travel to non-sensitive countries before your trip; however, keep a personal record of such travel for future clearance investigations.	52 days before trip. 37 days before trip. Prior to travel, or as soon as practical.	Foreign Travel

Supervisors' Reporting Requirements

In compliance with CPR400.3.7, *Security Concerns Reporting Process*, and DOE M 470.4-5, *Personnel Security*, all supervisors aware of the following conditions affecting a Member of the Workforce's access authorization status must provide notification of:

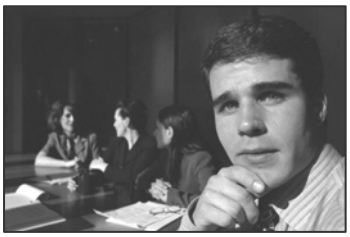
> An individual's hospitalization for a mental illness or other condition (e.g., substance or alcohol abuse) that may cause a significant defect in the individual's judgment or reliability. Verbal notification must be made within 8 working hours and written confirmation within the next 10 working days.

Information of Personnel Security Interest

Such information must be characterized as reliable and relevant and create a question as to an individual's access authorization eligibility as described in 10 CFR 710.8, *Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*.

CORPORATE INVESTIGATIONS

Waste, Fraud, and Abuse



You must be vigilant in protecting the funds and resources that are entrusted to Sandia by our government and customers.

Incidents of waste, fraud, and abuse, as well as criminal matters, must be reported to the Corporate Investigators (see contact lists on pages 34-39) and other appropriate authorities. The Sandia Ombuds and Ethics Offices are also available.

Theft of Property

Any theft of Sandia or U.S. Government property shall be reported immediately to the Corporate Investigators.

All property that is considered stolen, lost, or missing must be reported, regardless of value and regardless of whether it is considered controlled or uncontrolled property.

Wrongdoing

You must report incidents of wrongdoing to the Corporate Investigators.

You may also report directly to the Office of the Inspector General any information concerning wrongdoing by DOE employees, contractors, subcontractors, consultants, grantees, or other recipients of DOE financial assistance, or their employees.

Drugs in the Workplace

Illegal drugs are prohibited on both Sandia-controlled premises and Kirtland Air Force Base property. The use of illegal drugs is a serious offense and could result in termination of your clearance and eventually your employment, as well as arrest.

Incidents of illegal drugs in the workplace must be reported to the Corporate Investigators. This includes, but is not limited to, trafficking in, selling, transferring, possessing, or using illegal drugs.

Individuals who have illegally used or trafficked in a controlled substance in the past may be asked to sign a drug certification form in which they attest to refrain from using or being involved with illegal drugs while employed in a position requiring a security clearance.

Security Violations

Security violations are a criminal breach of federal law and can be acts of deliberate intent to harm national interests.

Severe criminal penalties, including termination, imprisonment, or both, may be imposed for security violations.

Sandia management is responsible for taking corrective action(s) and reporting any security violations in writing to the Corporate Investigators.

If you have questions or need details concerning security violations, consult the Corporate Investigators.

Suspension/Termination

Your access authorization may be suspended or terminated for any of, but not limited to, the following derogatory* reasons:

- Gross misconduct with, failure to protect, or careless handling of classified matter.
- Disclosure of classified information to a person unauthorized to receive such information.
- Failure to safeguard SNM.
- Theft of government property.
- Participation in or association with any act of sabotage, espionage, treason, terrorism, or sedition.
- Gross violation of or disregard for security or safeguards regulations.
- Illness or mental condition that significantly impairs judgment or reliability.
- Excessive or habitual use of alcohol.
- Trafficking in, selling, transferring, possessing, or using illicit drugs or controlled substances.
- Engaging in any unusual conduct that reveals you to be dishonest, unreliable, or untrustworthy.

*10CFR710.8, *Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*, lists information that is considered "derogatory." Such information casts doubt upon the reliability of a Member of the Workforce to obtain or maintain access authorization to DOE security interests.

CLEARANCE ACCESS AND BADGES

Clearance Access

Access refers to the ability and opportunity to obtain knowledge, use, or possession of classified information. Access is based on NTK, or need to access classified matter to perform official or contractual duties.

Clearance and Badge Types

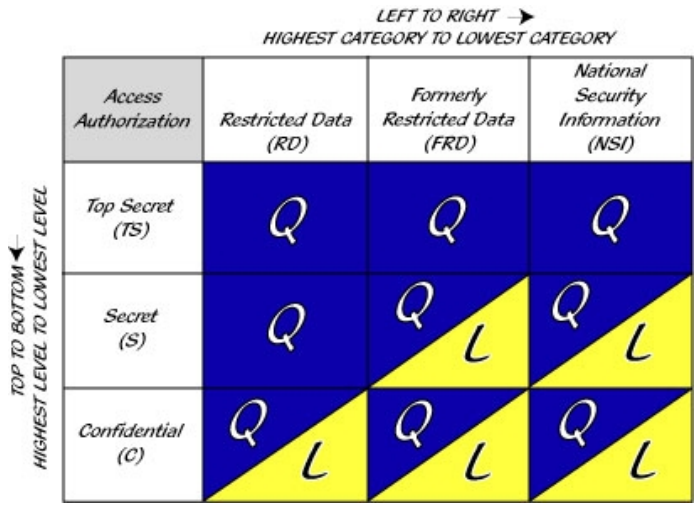
All Members of the Workforce are issued DOE standard badges that indicate their clearance level. The most common clearances granted by the DOE at SNL are "L" and "Q."

An "L" clearance (yellow badge) authorizes unescorted access to:

- Secret Formerly Restricted Data (SFRD).
- Secret National Security information (SNSI).
- Confidential Restricted Data (CRD).
- Confidential Formerly Restricted Data (CFRD).
- Confidential National Security Information (CNSI).
- SNM categories II and III.
- Unescorted access to Limited and Protected areas.

A "Q" clearance (blue badge) allows unescorted access to the information listed above, plus:

- Restricted Data (RD).
- Top Secret Restricted Data (TSRD).
- Secret Restricted Data (SRD).
- Top Secret National Security Information (TSNSI).
- SNM Category I (only if individual has Human Reliability Program [HRP] certification and NTK).



Your background will be reinvestigated:

- **Every 5 years** if you hold a "Q" clearance.
- **Every 10 years** if you hold an "L" clearance.

DOE badges in the automated systems at other sites do not work at SNL unless they have been enrolled at the Badge Office.

Your Responsibilities for Your Security Badge

The badge you will receive is an important credential—evidence that a rigorous background investigation found you trustworthy regarding our nation's security. Please familiarize yourself with the policies listed below.

- It is against the law to counterfeit, alter, or misuse your badge.
- If your badge is lost or stolen, report it immediately to the Badge Office (see contact lists on pages 34-39). Additionally, SA 2730-LSB, SNL Lost/Stolen Badge Report, must be completed and turned into the Badge Office prior to the release of a replacement security badge.
- Your badge is the property of DOE and must be returned to the Badge Office if it has expired, is no longer needed, or upon termination.
- Do not use your badge outside of DOE facilities, other than for government purposes. If you need an SNL ID, the Badge Office can supply you with one.
- If you take an extended leave of absence (90 days or longer), you must return your badge to the Badge Office.
- Upon entering any Limited area (LA), present your badge for examination by the Security Police Officer or use the automated access points.

In addition, you must:

- Wear your badge in plain view, above the waist while in DOE-owned or leased security areas, including Property Protection areas (PPAs).
- Renew your badge when your contract company or contract number changes.
- Renew your badge when your name or physical appearance changes.
- Renew your badge if faded or damaged.
- Remove your badge when off-site—for example, don't wear your badge to restaurants, or to obtain a gym or an airport parking discount.
- Protect your badge from theft.
- Protect your PIN at all times.
  - Do not write it down, or give it to others.
  - Shield the badge reader when entering your PIN.
  - If you suspect that your PIN has been compromised, contact the Badge Office to have it changed.

UNCLEARED PERSONS OR VISITORS

General Requirements

Uncleared visitors must wear a site-specific, grey-striped badge (Sandia-issued badges have a blue thunderbird on the lower part).

Uncleared U.S. citizens with appropriate DOE-approved badges may:

- Enter security areas if they are on official business and are appropriately escorted.

Escorting

Within Limited or more restricted areas, only a U.S. citizen with a "Q" or "L" clearance and DOE-approved badge may escort.

Your responsibilities as an escort anywhere on Sandia-controlled premises include:

- Do not escort more than eight uncleared persons.
- Brief escorted persons about evacuation procedures and how to report emergencies.
- Ensure that escorted persons are badged through the Badge Office.
- Inform escorted persons of prohibited items.
- Ensure that escorted persons follow rules and signs, including those relating to prohibited items.
- Ensure that escorted persons do not gain access to classified matter.
- Allow access by escorted persons through automated gates using your badge and personal identification number.
- If escort responsibility is transferred, ensure that new escorts are aware of their responsibilities.
- Ensure that escorted persons surrender their Sandia-issued badges per instructions on their orange card (SA 2730-CB) and that surrendered badges have been placed in a badge drop box or taken to the SNL Badge Office.

Escorted persons must remain with their escort at all times.

Vouching/Piggybacking

Vouching (a.k.a. piggybacking) is a term used to describe when one person allows another unescorted access.

When you vouch for another person, you accept the responsibility and consequences of allowing that person into the area.

When in doubt, refer persons who request vouching (a.k.a. "piggybacking" to the Badge Office.

Questions to Ask Yourself Before Vouching

- How well do I know this person?
- How much risk do I want to accept?
- Is the individual's badge failing to swipe because he or she:
  - No longer has a clearance but the badge was not confiscated?
  - Is wearing a badge that is frayed so badly that it will not swipe?

After considering the above, examine the individual's badge to ensure that:

- It is a DOE-approved badge.
- The badge photo matches the wearer.
- The badge has not been tampered with or altered in anyway.
- The badge has not expired.

For Your Information

For additional information on vouching or piggybacking, contact the Badge Office (see contact lists on pages 34-39) or see CPR400.3.11, *Access Controls*.

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM)

The purpose of the TSCM program is to:

- Identify exploitable security weaknesses and enhance technical and physical security.
- Detect, deter, and nullify unauthorized clandestine technical intelligence collection that could compromise classified NSI, RD, FRD, and/or UCI.
- Ensure that any overt surveillance complies with CPR400.3.1, *Technical Surveillance – Audio and Video Recording*.

Your Responsibilities

Your TSCM responsibilities include reporting suspected or clandestine audio or video equipment immediately, and taking the following steps:

1. Stop all classified or sensitive discussions.
2. Secure the area so that no one can remove or modify the device.
3. Contact the TSCM Team (see contact lists on pages 34-39) from a location outside the area.
4. For additional information, consult the TSCM section of CPR400.3.1, *Technical Surveillance – Audio and Video Recording*.

Technical Surveillance Equipment (TSE)

TSE is commonly developed for law enforcement (e.g., wireless microphones worn on the body or miniature cameras inserted in clocks). This equipment allows law enforcement personnel to surveil criminal activity.

Some operations at SNL use equipment that is capable of being used as TSE in its "as purchased" state, even though it was acquired for legitimate business needs. This includes wireless microphones, wireless cameras, and radio-frequency transmitters. Areas with active surveillance equipment have signs posted to inform Members of the Workforce of its presence, and owners of such devices are required to develop and maintain special security plans. For additional requirements associated with TSE, consult CPR400.3.1, *Technical Surveillance – Audio and Video Recording*.

Potential Technical Surveillance Equipment (PTSE)

PTSE includes some commercial equipment that could be used as surveillance equipment, even though it's not expressly designed to function that way. In general, PTSE must be registered with TSCM, according to CPR400.3.1, *Technical Surveillance – Audio and Video Recording*.

The following list of PTSE is not comprehensive, but is included here for guidance only.

Digital cameras	35mm cameras
Video cameras	Microphones
Portable scanning devices	Portable digital assistants (PDAs) with digital camera or audio recording attachments
MP3 players	Dictaphones and digital voice recorders

Equipment that is maintained or installed in a Sandia-owned or -controlled PPA is exempt from registration requirements. Local line management may institute their own control and inventory methods for equipment. Equipment that is stored, maintained, or installed in a Limited or more restricted area must be controlled according to CPR 400.3.1, *Technical Surveillance – Audio and Video Recording*.

If the equipment is not covered by another CPR and is not exempt, register PTSE by using SF 2925-TSE, Registration of Potential Technical Surveillance Equipment (Potential TSE), or a specially developed plan.

Cell Phones

While all cell phones, regardless of ownership, are prohibited within Limited and more restricted areas, some exceptions may be granted under certain circumstances. Regardless of ownership, cell phones may be carried and used in PPAs unless local restrictions apply. All users must comply with line- and site-specific rules and restrictions.

All Sandia-purchased cell phones:

- Must have a blue Sandia property sticker affixed.
- Must be turned off (preferably with the batteries removed) unless properly registered, using SF 7643-USE, Cellular Phone Critical Use.
- May be used only as necessary for safety and security reasons in support of critical operations, or to report an emergency (844-0911).

Cell Phones and Classified/UCI Discussions

Members of the Workforce must:

- **Not** discuss classified or unclassified controlled information on cell phones.
- Meeting coordinators should remove all cell phones from conference or other rooms where classified matter is being processed or discussed, or may be discussed.

Do **not** discuss classified information outside Limited Areas (Las). Never discuss classified or UCI over a non-secure telephone or near an in-use telephone.

Cell Phones and Security Areas

Cell Phones / Security Area	Privately Purchased	Sandia-Purchased	Non-Sandia, Government-Purchased
PPA	Permitted only under special circumstances (e.g., medical reasons) *Form Needed:* SF 7643-POC, Cellular Phone Approval—Non-Government Phones Within SNL Limited and Protected Areas	Permitted with prior authorization *Forms Needed:* SF 7643-PUR, Sandia-Purchased Cellular Phone Security Registration SF 7643-USE-Cellular Phone Critical Use	Permitted with prior exception *Form Needed:* SF 7643-OTE, US Government Agency Visitor One-Time Exception to SNL Cellular Telephone Requirements
Limited Area	Permitted only under special circumstances (e.g., medical reasons) *Form Needed:* SF 7643-POC, Cellular Phone Approval—Non-Government Phones Within SNL Limited and Protected Areas	Permitted with prior authorization. *Forms Needed:* SF 7643-PUR, Sandia-Purchased Cellular Phone Security Registration SF 7643-USE-Cellular Phone Critical Use	Permitted with prior exception *Form Needed:* SF 7643-OTE, US Government Agency Visitor One-Time Exception to SNL Cellular Telephone Requirements
Protected Area	Permitted only under special circumstances (e.g., medical reasons) *Form Needed:* SF 7643-POC, Cellular Phone Approval—Non-Government Phones Within SNL Limited and Protected Areas	Prohibited.	Permitted with prior exception *Form Needed:* SF 7643-OTE, US Government Agency Visitor One-Time Exception to SNL Cellular Telephone Requirements

For additional information, see CPR400.3.16, *Cellular Phones*.

Personal Data Assistants (PDAs) and Pagers

Personally owned small electronic items (e.g., PDAs, and pocket PCs) are not permitted in Limited or more restricted areas.

Sandia- or government-purchased small electronic items are permitted in Limited areas but must be identified with a blue Sandia property sticker. Some security areas require TSCM inspection of PDAs before they are permitted in the areas.

PDAs with recording capability (e.g., modem, microphone, camera) must be registered with TSCM using a security plan or SF 2925-TSE, Registration of Potential Technical Surveillance Equipment, if the recording feature has not been disabled or is going to be used in the course of work.

PDAs with radio frequency (RF)-transmitting capability must have the transmitting capability disabled before entering Limited or more restricted areas. If the wireless feature is to be used in the course of work, contact the Wireless Infrastructure Project for authorizations.

Pagers with transmitting capabilities are not permitted in Limited areas and PPAs.

Sandia-purchased BlackBerry devices are not allowed in Limited areas.

CYBER SECURITY

You are responsible for protecting the computer(s) you use at work, and for protecting any information generated on computers from waste, fraud, and abuse. Cyber Security is an integral component of protecting classified matter at SNL.

You must:

- Process UCI and classified data on authorized computers only.
- Comply with copyright and licensing restrictions.

You may not:

- Play games on or use computers for other personally owned applications.
- Destroy or modify hardware, software, or data without authorization.

For Your Information

For more information on Cyber Security, or if questions arise, consult your Cyber Security Representative in the Cyber Security Services and Technologies Department (see contact lists on pages 34-39).

SECURITY INCIDENT MANAGEMENT PROGRAM (SIMP)

Reporting Security-Related Concerns

All incidents of security concern (e.g., any or suspected noncompliance that affects or potentially affects SNL security) should be reported promptly. This ensures containment of potential damage, timely and appropriate reporting, and follow-up. Do **not** discuss details of an incident via telephone, alphanumeric pager, e-mail, or voice-mail. See the list on pages 34-39 for contact information.

After a Security Incident

After an incident, Members of the Workforce must take steps to prevent further compromise of government information or property:

- Preserve and protect evidence related to an incident in a manner that is appropriate for the level of classification.
- For classified matter, take action to preclude further compromise or potential compromise when it is determined that information may have been lost, compromised, or is otherwise unaccounted for.
- For unclassified computer concerns (e.g., unauthorized access, viruses, junk e-mail/spam), take action to preclude further compromise or potential compromise of affected systems.
- For prohibited articles, take action to preclude further compromise or potential compromise by making the article safe, or by turning the article off and removing batteries.

Managers are responsible for ensuring that an investigation begins immediately upon discovery that classified matter may be lost or unaccounted for.

During an Investigation

During investigation or pre-investigation activities, Members of the Workforce must cooperate with SIMP Inquiry Officials and other security program management as they conduct fact-finding inquiries. Do not personally investigate incidents.

Infractions

Security infractions are issued in response to a breach of DOE or Sandia security rules, whether deliberate or because of carelessness or ignorance. An infraction could be issued for any of the following reasons (this list is not all-inclusive):

- Leaving a classified repository unattended or unsecured.
- Failing to account for classified matter.
- Failing to maintain prescribed records for accountable classified matter.
- Removing classified matter from a security area without proper authority.
- Discussing classified information over unsecured telephones.
- Not obtaining classification guidance, thus causing compromise of classified information.

- Failing to properly mark classified matter as determined by a classification authority.
- Improperly destroying classified matter.
- Improperly transmitting classified matter.
- Improperly escorting uncleared visitors in security areas.
- Introducing prohibited items into security areas.
- Bringing a prohibited item into a Limited area.

Penalties for Security Infractions

All infractions are reported to DOE. Corrective actions are always required and must be reported in writing to SIMP, so that they can be forwarded to DOE.

At SNL/CA, the necessary form will be completed by Security personnel.

Disciplinary actions are at the discretion of management, and range from coaching and counseling to suspension or termination. When the infraction is committed by a Sandia employee, his or her supervisor is responsible for applying disciplinary actions. When the infraction is committed by a contractor, management at the contracting company is responsible for discipline.

MEDIA RELATIONS

Public media reports of classified work at SNL should not be affirmed, denied, or commented upon.

Requirement associated with media relations can be found in CPR200.1.1, *Media Relations*.

SECURITY CONTACTS, SNL/NM

FUNCTION/CONTACT	PHONE	TECH WEB KEY WORDS
Access Control/Badges		
Bob Schwartzman (Badge Office)	844-1206	"Badge Office"
After hours	844-3155	
Help Line	284-3626	
Briefings		
Charles Montoya	844-2697	"Security Awareness Home"
Fran Armijo	284-2416	
Classification		
Bruce Green	844-2490	"Classification"
Classified Matter Protection & Control		
Dennis Connors	844-4834	"CMPC"
Clearance Reinvestigations		
Angela Chavez	844-1975	"Reinvestgiations"
Consultant Badging		
Kristy Kaneshiro	844-4493	"Consultant Clearances"
Corporate Investigations		
Pat O'Neill or Mark Ludwig	845-9900	"Corporate Investigations"
Counterintelligence		
Cal Guymon	844-4288	"Counterintelligence"
John Hudenko	284-4894	
Cyber Security		
Sharon Walsh	844-2322	"Cyber Security"
Ethics and Ombuds	844-1744	"Ethics Ombuds"
Escorting		
Bob Schwartzman	844-1206	"Escorting"
Help Line	284-2636	
Export/Import Control		
Steve Sultemeier	844-7112	"Import/Export"
Foreign Travel		
Help Line	844-1300	"Foreign Travel"
Marcie Jordan	845-8488	

Function/Contact	Phone	Tech Web Key Words
Foreign Visits and Assignments		
Help Line	844-1300	"Foreign Visits"
Mail and Shipping Channels		
Sharon Gorman	844-8952	"Classified Shipping"
Marriage Reports and Cohabitation		
Melanie Heyborne	284-9519	"Marriage"
Caren Calvin	284-9773	
Media Relations		
Iris Aboytes	844-2282	"Lab Communications"
Medical		
OPSEC		
Reggie Tibbetts	844-5244	"OPSEC" or "Operations Security"
Micky Hogue	844-6640	
Protective Force		
North Desk Lieutenant	844-3155	"Proforce"
South Desk Lieutenant	845-3394	
Reporting Requirements (e.g., citizenship changes, name changes, marriage, and cohabitation)	**284-3103**	**"Reporting Requirements"**
Security Awareness		
Charles Montoya	844-2697	"Security Awareness Home"
Fran Armijo	284-2416	
SIMP/Security Incident Management Program	**540-2382 (pager)**	**"SIMP"**
Technical Security		
Bruce Behrends	**284-6537**	"Technical Security"
TSCM/Technical Surveillance Countermeasures		
Sam Holmes	845-9345	"Surveillance"
Terminations		
Kristy Kaneshiro	844-4493	"Personnel Security"

SECURITY CONTACTS, TTR

FUNCTION/CONTACT	PHONE	TECH WEB KEY WORDS
Marriage Reports and Cohabitation		
Nikki Zimmerman	295-8336	"Marriage"
Media Relations		
Iris Aboytes	505-844-2282	"Lab Communications"
Medical		
Bruce Riley	295-8404	"Medical"
Betsy Riley	295-8345	
OPSEC		
Steve Feador	295-8219	"OPSEC"
Protective Force		
Ralph Garcia	295-8285	"ProForce"
Security Awareness		
Anthony Pagano	295-8113	"Security Awareness Home"
SIMP/Security Incident Management Program	**505-540-2382 (pager)**	**"SIMP"**
Technical Security		
Gene Littlefield	295-8324	"Technical Security"
TCSM/Technical Surveillance Countermeasures		
Sam Holmes	(505) 845-9345	"Surveillance"
Terminations		
Kristy Kaneshiro	(505) 844-4493	"Personnel Security"

FUNCTION/CONTACT	PHONE	TECH WEB KEY WORDS
Access Control/Badges		
Nikki Zimmerman	295-8336	"Badge Office"
Briefings		
Anthony Pagano	295-8113	"Security Awareness Home"
Classification		
Karl Hess	295-8187	"Classification"
Steve Feador	295-8219	
Gene Littlefield	295-8324	
Classified Matter Protection & Control		
Dennis Connors	505-844-4834	"CMPC"
Clearance Reinvestigations		
Angela Chavez	505-844-1975	"Reinvestgiations"
Consultant Badging		
Kristy Kaneshiro	505-844-4493	"Consultant Clearances"
Corporate Investigations		
Pat O'Neill or Mark Ludwig	505-845-9900	"Corporate Investigations"
Counterintelligence		
Cal Guymon	505-844-4288	"Counterintelligence"
John Hudenko	505-284-4894	
Cyber Security		
Sharon Walsh	505-844-2322	"Cyber Security"
Ethics and Ombuds	505-844-1744	"Ethics Ombuds"
Escorting		
Anthony Pagano	295-8113	"Escorting"
Nikki Zimmerman	295-8336	
Export/Import Control		
Steve Sultemeier	505-844-7112	"Import/Export"
Foreign Travel		
Help Line	505-844-1300	"Foreign Travel"
Marcie Jordan	505-845-8488	
Foreign Visits and Assignments		
Help Line	844-1300	"Foreign Visits"
Mail and Shipping Channels		
Judy Ripley	295-8273	"Classified Shipping"

SECURITY CONTACTS, SNL/CA

FUCTION/CONTACT	PHONE	TECH WEB KEY WORDS
Access Control/Badges		
Badge Office	294-1358	"CA Badge Office"
After hours (Security)	294-2300	
Briefings		
Dionne Hidalgo	294-4649	"Security Awareness"
Classification		
Winalee Carter	294-2202	"CA Classification"
Classified Matter Protection & Control		
Heather EgtervanWissekerke	294-3160	"CA CMPC"
Clearance Processing		
Carol James	294-2061	"CA Badge Office"
Corporate Investigations		
Pat O'Neill or Mark Ludwig	845-9900	"Corporate Investigations"
Counterintelligence		
David Massone	294-6199	"CA Counterintelligence"
Frances Moore	294-6111	
Cyber Security		
Scott Maruoka	294-2558	"CA Cyber Security"
Ethics and Ombuds	844-1744	"Ethics Ombuds"
Escorting		
Theresa Price	294-3043	"CA Escorting"
Export/Import Control		
Winalee Carter	294-2202	"CA Import/Export"
Foreign Travel		
Help Line	844-1300	"Foreign Travel"
Marcie Jordan	845-8488	
Foreign Visits and Assignments		
Pat Lull	294-3042	"Foreign Visits"

Function/Contact	Phone	Tech Web Key Words
Mail and Shipping Channels		
Nancy Morris	294-2980	"CA Classified Shipping"
Marriage Reports and Cohabitation		
Carol James	294-2061	"Marriage"
OPSEC		
Michelle Smith	294-2454	"CA OPSEC" or "CA Operations Security"
Protective Force		
Central Alarm Station	294-2300	"CA Proforce"
Security Awareness		
Dionne Hidalgo	294-4649	"CA Security Awareness"
SIMP/Security Incident Management Program	**888-932-9710 (pager)**	**"CA SIMP"**
Technical Security		
Rick Maurer	294-2975	"Technical Security"
TSCM/Technical Surveillance Countermeasures		
Lyle Hansen	294-1284	"Surveillance"
Terminations		
Carol James	294-2061	"Personnel Security"

Security Briefing Review

Please complete this form and hand it in with the puzzle.

Last _____ First _____ MI _____

Signature _____ Date _____

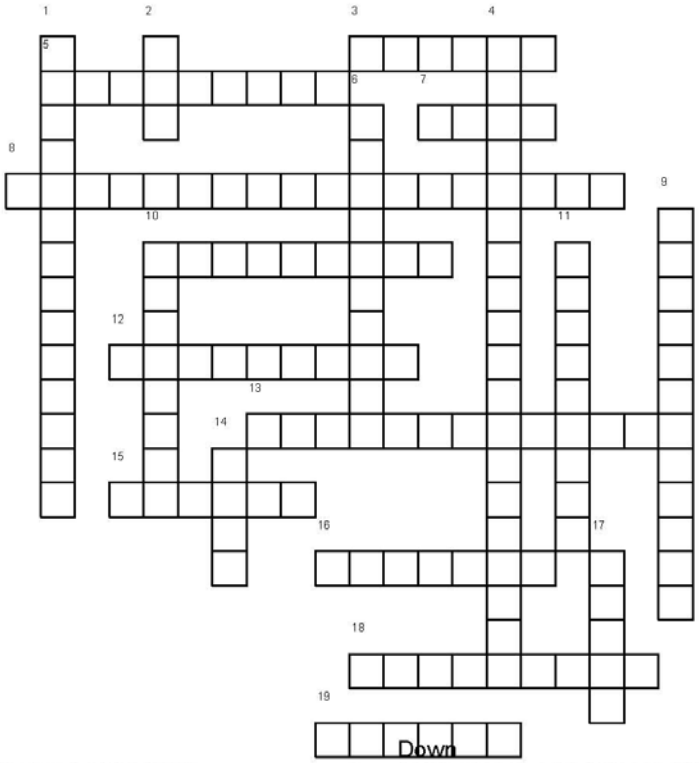
Company/Org. _____ Last digits of SSN _____

☐ Employee ☐ Contractor ☐ Consultant ☐ Student ☐ KMP

☐ New ☐ Reinstate

Security Comprehensive Briefing

Test your knowledge of what you have discovered about Sandia National Laboratories and its areas of security.



Across

3 The ProForce members may do this upon entering or leaving Sandia-controlled premises of all personnel and their hand-carried items or vehicles
5 What is the second part of answer to SF312
7 Q-cleared individual, access authorized up to SRD with a need to know has what color badge
8 What area is established for the protection of DOE property
10 Travel to____countries must be reported through the corporate Travel Information System as soon as possible
12 Incidents of illegal drugs in the workplace shall be reported to which investigators
13 What is the agreement between you and the federal government called (first part)
15 Unauthorized disclosure of what could reasonably be expected to cause serious damage to national security
16 A security area having boundaries identified by barriers for the protection of classifed information
18 Unauthorized disclosure of what could reasonably be expected to cause exceptionally grave damage to national security
19 L-cleared, access authorized up to SFRD with need to know has what color badge

Down

1 What area is established for the protection of special nuclear material
2 Uncleared foreign national, no classifed access has what color badge
4 Which office must you notify if you received unsolicted e-mail from a sensitive country foreign national
6 Personally owned cell phones, PDAs, iPods, Blackberries, thumb drives are examples of
9 Unauthorized disclosure of what could reasonably be expected to cause undue risk to the common defense and security
10 Special Nuclear Material like enriched uranium or plutonium must be guarded to prevent possible theft or ___
11 Another type of security area requiring additional need to know authorization
14 Uncleared US citizens, no classifed access, requiring escort in Limited areas have what color badge
17 To make sure you don't inadvertantly release information to potential adversaries, always remember to practice--

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.2, 1.3, and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, * the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.

Reset

STANDARD FORM 312 (Rev. 1-00)
Prescribed by NARA/ISOO
32 CFR 2003, E.O. 12958

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military): Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER *(See Notice below)*

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or print)*

WITNESS		**ACCEPTANCE**	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		**THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.**	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS *(Type or print)*		NAME AND ADDRESS *(Type or print)*	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS *(Type or print)*	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

Reset

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.