Initial Security Briefing

This briefing paper sets forth certain basic Federal rules and regulations and provides some administrative information concerning the security program to assist you in fulfilling your responsibility to safeguard national security information.

Although this briefing is oriented to the type of access to national security information anticipated in your present University assignment, the principles, safeguards and regulations mentioned herein apply to any access to national security information. Should you at any time become or foresee requiring access to information for which you are not currently cleared, you should contact the University Research Security Officer or Assistant Research Security Officer and inform them of the details without delay. You then may be provided with additional information you need.

Within the University of California system, the responsibility for coordinating the University-wide research security program and for conducting the headquarters security program has been delegated to the University Research Security Officer in the Office of the President of the University. A campus may have a Security Officer responsible for the research security program at a particular campus facility. These security officers are available to assist you with security matters and give you any additional security briefings related to that campus facility, should circumstances require it.

Because security clearance investigations and other security correspondence may touch on personal or private information, arrangements have been made for all correspondence addressed to the University Research Security Officer or Assistant Research Security Officer (may also be referred to as Facility Security Officer and Assistant Facility Security Officer), by name or by title, to be delivered directly to the Security or Assistant Security Officer unopened. Paper security files are kept in locked cabinets. Electronic information is appropriately encrypted and maintained on systems not accessed outside of the Research Security Office. Although any information forwarded in connection with security matters is given appropriate protection every effort is made to minimize the amount of personal information maintained in either paper or electronic form. The following address is a recognized address for this purpose:

University Research Security Office
Laboratory Management Office
University of California Office of the President
1111 Broadway St., 14th Floor
Oakland, CA 94607-4180
Phone: (510) 987-9846

The University Research Security Office does not issue individual certificates or identification cards indicating that a clearance has been granted to you. Depending on the frequency and need for access to facilities possessing classified information, you will be issued a temporary badge by various Federal/contractors at physical sites where you visit at the time or your visit, or it will be requested that you be issued a federal credential (HSPD-12) through the Department of Energy that is accepted at most federal/contractor locations.

To visit a facility where national security information is to be discussed, or where classified objects may be observed, approval must first be obtained from the Federal agency concerned. This is accomplished by means of a "Visit Request". Unless you have been issued an appropriate badge authorizing your visit, the "Visit Request" is prepared/coordinated in my office and is forwarded through official channels of the controlling Federal agency to the installation to be visited.

In connection with the granting of access to national security information, the Government requires that reports be submitted in certain situations. Normally, the reports will be made by the Research Security Officer on behalf of the University.

To enable the University Research Security Officer to make the required reports, persons holding a University of California-sponsored security clearance must notify the University Research Security Officer if they have a reportable issue (see section on reporting requirements).

Security clearance holders may be targets of interest by foreign governments and entities. Travel to foreign countries exposes clearance holders to some additional risk of contact, surveillance or influence beyond that which may be accomplished in this country. Accordingly persons with security clearances have some reporting and briefing/debriefing requirements associated with foreign travel (see section on requirements for Foreign Travel).

Security clearances issued through the sponsorship of the University are used in connection with University business and specific assignments. It is required that these security clearances be terminated when you sever your present relationship or assignment with the University. When your clearance is terminated you will be briefed on the necessity to continue to protect any national security information known to you, and you will be required to complete a Security Termination Debriefing Statement on the bottom of Form SF 312 (Non-disclosure Agreement).

For better understanding of your involvement with national security information, some definitions are included with the regulations and safeguards that follow.

OVERVIEW IF THE SECURITY CLASSIFICATION SYSTEM

The University of California performs classified contracts, is a member of joint ventures performing classified contracts, and have employees who receive and/or generate classified information.

What does a security clearance mean?

A security clearance (access authorization) means that you are eligible to be granted access to classified information or material at the level of **TOP SECRET**, **SECRET**, or **CONFIDENTIAL**, based on the extent of your background investigation and based on your NEED TO KNOW, as related to your assigned responsibilities.

DEFINITIONS OF CLASSIFIED INFORMATION

For a better understanding of your involvement with classified information when you visit the national security laboratories, some helpful definitions follow:

Classified Information: Any information that requires protection against unauthorized disclosure in the interest of the national defense and security or foreign relations of the United States pursuant to applicable U.S. Statute or Executive Order. The term includes:

a. Restricted Data
b. Formerly Restricted Data
c. National Security Information

Included within each of the above designations are three categories indicating degrees of importance, denoted by Top Secret (TS), Secret (S) and Confidential (C).

***Top Secret*—**the highest level applied to information whose unauthorized disclosure could be expected to cause *exceptionally grave* damage to the national security of the United States.

***Secret*—**the classification level between Confidential and Top Secret whose unauthorized disclosure could be expected to cause *serious* damage to the national security of the United States.

***Confidential*—**the lowest level applied to information whose unauthorized disclosure could be expected to cause damage to the national security of the United States.

***Restricted Data*—**Data defined in Section 11.y. of the Atomic Energy Act of 1954, as amended, 42 U.S.C. § 2014(y), as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special

nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142."

Formerly Restricted Data—Classified information jointly determined by the Department of Energy (or its predecessors the Atomic Energy Commission and the Energy Research and Development Administration) and the Department of Defense to be related primarily to the military utilization of atomic weapons, and removed by DOE from the Restricted Data category pursuant to Section 142(d) of the Atomic Energy Act of 1954, as amended, 42 U.S.C. § 2162, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

National Security Information—Information that requires protection in the interest of national defense or foreign relations of the United States, that does not fall within the definition of Restricted Data or Formerly Restricted Data, and that is classified in accordance with an Executive Order.

Sigma Weapon Data Categories—In the 1980's DOE recognized the need for additional controls over certain Restricted and/or Formerly Restricted Data now detailed in 15 categories that concern the design, manufacture, or utilization of atomic weapons, or utilization of atomic weapons or nuclear explosive devices. This system is still in use today.

Classified Information "Need-to-Know" Principle—An individual seeking access to specific classified information has the obligation to explain his "need-to-know" to the holder of that information. The individual may not demand disclosure if the holder remains unconvinced with respect to "need-to-know." Disagreements will be resolved through management review.

Special Laboratory Briefings at Nuclear Weapons Laboratories—Frequently the Laboratory Management Office within the UC Office of the President assists with arranging visits and briefings at the Los Alamos and Lawrence Livermore National Laboratories for Regents and key UC management personnel. Those visits usually require special briefings by the Lab Use Control Site Coordinator for access to compartmentalized information (Sigmas 14 and 15).

ACCESS REQUIREMENTS

For obvious reasons, correspondence informing a person that a security clearance has been granted to him/her is not acceptable as evidence that the clearance is still valid at a later date. When it is appropriate for you to discuss classified information with other persons, their clearance status first must be verified through official sources. These sources include the University Research Security Officer, the Security Officer of the installation of the prospective recipient of the information, and the personnel security section of the Federal agency involved.

Classified discussions can only take place when the participants are physically at a location approved for classified discussions. Even there, care must be exercised when discussing classified information to preclude being overheard either by persons not a party to the discussion, or by a recording device, or a transmitting device such as a telephone in use. If classified discussions occur between persons at different locations, each participant must be in an approved facility for classified discussions and the method of transmitting voice and/or images must be on approved encrypted transmission devices.

Whenever classified information is being discussed, the parties to the discussion must be informed of the classification of the information ("SECRET") and of any additional markings involved (e.g., "Restricted Data", etc.). Special arrangements must be made for meetings and conferences involving discussions of classified information. These arrangements must be approved by the Federal agency involved, and considerable preparation is required.

Classified matter, properly sealed and without external indication of its contents, may be carried by an individual under certain conditions, but it must be placed in approved containers when not in use and for overnight storage. Information relative to approved containers and the conditions that must be met for carrying or mailing classified information can be obtained from the University Research Security Officer or from Security Officers of other installations handling classified matter. In unusual circumstances you may contact any security or intelligence activity of the Federal agency involved for information and assistance. Should you have classified matter which cannot be given proper storage, it should be torn and burned completely by you, and the ashes should be stirred and broken up. If you received the material from an official source, another cleared person should witness the act and a report must be made to the Security Officer of the source from which the material was received. National security classified documents, regardless of their source, received by individuals in connection with University affairs are required to be entered into the University's control system. The Research Security Officer should be contacted immediately if such documents are received. At all times you should avoid making notes which contain classified information because they will require the same special handling and storage as any other classified information. You should report any loss or possible compromise of classified documents or materials.

Even with the break-up of the Soviet Union and the end of the cold War, no nation has done away with its intelligence service. Some have changed their methods, but they still are all there. What are

they doing? The same thing they always did--collecting information in support of their national interests.

REPORTING REQUIREMENTS

The University Of California is committed to maintaining a security-conscious culture in which access to vital national security facilities and information is recognized as a privilege. Maintaining that privilege requires each individual to fully understand and fulfill the security obligations associated with his or her clearance (a.k.a. "access authorization").

Reporting requirements are significant obligations that each cleared individual must implement. Generally, this involves both an oral and a written report. An oral report has to be made to the Research Security Officer within 2 working days of the incident with a written report within 3 working days thereafter.

Your Responsibilities

Violations of the Law Within or Outside of the United States
If you are arrested, subject to criminal charges (including charges that are dismissed), or are detained by federal, state, or other law-enforcement authorities. **Note:** traffic violations for which only a fine of **$250.00 or less** was imposed do **not** have to be reported, unless the violations were drug or alcohol related.

Contacts with Foreign Nationals
You must immediately report substantive contact with any foreign national. **Note:** Contact is defined as "a substantive professional or personal relationship other than family members." Substantive is defined as "a relationship that is enduring, involves substantial sharing of personal information and/or the formation of emotional bonds."

Drugs and Intoxicants
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 must be reported to the Research Security Officer. This includes, but is not limited to, trafficking, selling, transferring, possessing, or using illegal drugs. Individuals who illegally used or trafficked a controlled substance may be asked to sign a drug certification form attesting to their commitment to refrain from using or being involved with illegal drugs while employed in a position requiring a security clearance. **Note:** You are not precluded from reporting information directly to the DOE Personnel Security Department.

Travel
You are required to report the following travel to the Research Security Officer:

- DOE-funded travel to a sensitive country.
- DOE-funded travel to a non-sensitive country.

- Personal foreign travel to a sensitive country.

Note: While you are not required to report personal foreign travel to a non-sensitive country, you should keep a personal record of such travel for future clearance (re)investigations.

Hospitalization You must report when you are hospitalized for mental illness, or other condition (e.g., drug or alcohol abuse) that may cause significant defect in your judgment or reliability.

Additional Reporting Requirements

Bankruptcy
Wage garnishment
Citizenship changes
Name change
Marriage and cohabitation
Clearance termination
Derogatory information
Waste, fraud, and abuse

UC, DOE and DoD Hotlines

Anyone, who witnesses what he or she believes to be a violation of ethical standards and/or the law, including but not limited to fraud, waste, or abuse of authority, potential leaks of classified information, or potential acts of terrorism, should report such conduct. The report can be made anonymously either to UC, DOE or DoD. Information of who and how to make a report to UC is attached; reports to DOE are to be made directly to the Inspector General of the Department of Energy Hotline at (800) 541-1625 (e-mail: ighotline@hq.doe.gov) and reports to the Department of Defense are to be made directly to the Inspector General of the Department of Defense Hotline at (800) 424-9098 (e-mail: hotline@dodig.mil)

REQUIREMENTS RELATING TO FOREIGN TRAVEL

Security clearance holders may be targets of interest by foreign governments and entities. Travel to foreign countries exposes clearance holders to some additional risk of contact, surveillance or influence beyond that which may be accomplished in this country. Accordingly persons with security clearances have some reporting and briefing/debriefing requirements associated with foreign travel:

Travel is	*Location includes*	*Approval is*	*Reporting is*	*Pre-travel briefing is*	*Post-travel de-briefing is*
Personally or privately funded or University funded, but not DOE contract funds[1]	Only non-sensitive countries	Not Required	Included in SF 86 (QNSP) at time of reinvestigation	Discretionary – may be requested by traveler	Required only if suspicious contact made
Personally or privately funded	Sensitive countries[2]	Not Required	To Research Security Office prior to travel	Discretionary – may be requested by DOE counterintelligence officer	Required only if suspicious contact made
University-	Any	Required[3]	To Research	Mandatory	Mandatory

[1] A trip is not "DOE contract" funded unless it is charged as a direct cost to Contract No. DE-AC02-05CH11231 for the management and operation of the Earnest Orland Lawrence Berkeley National Laboratory.

[2] See http://labs.ucop.edu/ for a list of sensitive countries.

[3] Must comply with DOE requirements under DOE O 551.C, Official Foreign Travel. All foreign travel requests must be entered into FTMS within 45 calendar days before the departure date if travel is to a sensitive country or involves a sensitive subject. For the convenience of the traveler, DOE F 551.1, *Request For Approval For Foreign Travel*, can be completed and provided to the University's Research Security Officer for review and forwarding on to the appropriate DOE Counterintelligence Officer for entry into the FTMS.

funded with DOE contract funds[1]	foreign country		Security Office 60 days prior to travel[4]		

In addition to the requirement listed above, travelers with laptops and other data storage devices need to be sensitive to requirements associated with export controls and personally identifiable information. Foreign travel represents an increased risk that data storage devices may be stolen or "mirrored".

[4] UC employees assigned to work at the Earnest Orland Lawrence Berkeley National Laboratory follow the procedures at http://travel.lbl.goc/foreign to obtain required DOE foreign travel approvals.

ACKNOWLEDGEMENT OF BRIEFING

TO: University Research Security Manager
Laboratory Management Office
University of California
1111 Broadway Street, Suite 1450
Oakland, CA 94607-4180

Receipt of a copy of the initial security briefing is hereby acknowledged.

DATE: _____

PRINT NAME: _____

SIGNATURE: _____
