UNIVERSITY Of CALIFORNIA

2012 Annual Security Refresher Briefing

Lawrence Livermore National Laboratory

Los Alamos National Laboratory

Protecting Our America~Your National Laboratories

University of California, Office of the President, 1111 Franklin Street, Oakland, CA 94607

Introduction

Objective

The objective of the University of California's Annual Security Refresher Briefing is to remind individuals of their safeguards and security responsibilities and to promote continuing awareness of good security practices. This briefing also helps employees develop an appreciation for the need to protect our country's national security interests.

As the federal security regulations require, the annual security refresher briefing addresses site-specific issues and selectively reinforces other information.

U.S. Department of Energy (DOE) Manual 470.4-1 Section K, "Safeguards and Security Awareness Program," requires that "Cleared individuals must receive annual (at least every twelve months) refresher briefings".

In addition, the National Industrial Security Program Operating Manual (NISPOM) dated January 1995 prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information. Paragraph 3-107 of the NISPOM dictates, "The contractor shall provide all cleared employees with some form of security education and training at least annually. The refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared employees informed of appropriate changes in security regulations. Contractors shall maintain records about the program offered and employee participation in them".

This briefing has four main sections:

- Identifying Classified Information.
- Reporting Requirements.
- Classified Matter Protection and Control.
- Counterintelligence, Threat Awareness and OPSEC.

Target Audience

The University sponsors clearances for three different groups:

- Regents (whose designation as "key management personnel" require them to be cleared or formally excluded from classified matters in accordance with federal requirements).
- University employees and consultants involved in oversight of University classified contracts or joint ventures.
- University employees performing work requiring access to and/or creation of classified documents.

This briefing is designed to cover only security requirements applicable to all three groups and to provide links and references to more detailed information relevant to a single group.

Your Responsibility

We encourage you to carefully review the material in this briefing (and references to specialized situations that may be applicable to you) to better understand various security issues, initiatives and policies applicable to your University-sponsored security clearance.

Acknowledgment of Briefing

Please acknowledge your 2012 refresher briefing by **October 30, 2012**. This briefing is an annual requirement by DOE and DoD. Failure to do so could result in administrative actions determined by DOE, including possible administrative termination of the security clearance, until such a time as the individual has complied with the briefing requirement.

Ronald A. Nelson
Research Security Officer
and Special Assistant, Contracts & Administration
Laboratory Management Office
University California Office of the President

Section 1:
Identifying Classified Information

Objectives

After successfully completing this section, you will be able to:

- Recall the Security Classification System.
- Understand the role of "Need to Know".

The Security Classification System

The University of California performs work under classified contracts, is a member of joint ventures performing classified contracts (the Los Alamos National Security LLC and Lawrence Livermore National Security LLC), and has employees who receive and/or generate classified information.

Levels And Categories of Classified Information

Classified information is designated by both a classification level and a category. The classification level is based on how much our national security could be damaged if the information were to be released to unauthorized person(s). There are three classification levels:

Top Secret (TS)— 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 (S)— 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 (C)— the lowest level applied to information whose unauthorized disclosure could be expected to cause *damage* to the national security of the United States.

The Security Classification System

The classification category describes the type of information contained in the material.

There are three classification categories:

Restricted Data (RD) — 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 (FRD) — 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 (NSI)— 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 by the President of the United States.

Need to Know

Need to know (NTK) is the determination by an authorized holder of classified information that access to the information is required by another appropriately-cleared individual in order to perform official duties.

You may need to make "Need To Know" decisions when:

- Someone wants to view a document under your control.
- You are briefed on a very sensitive project.
- Discussing specific projects.

Although someone may have a clearance - **they may not have the NEED TO KNOW.** If you have any doubt, ask your supervisor or contact the UC Research Security Office.

Section 2:
Reporting Requirements

Objectives

After successfully completing this section, you will be able to:

- Identify the activities or situations that you are required to report in order to maintain your DOE security clearance.
- Recall the Reporting Requirements for Foreign Travel.
- Identify Incidents of Security Concern.
- Understand the process for Leaves of Absences and Terminations.
- Recall the UC, DOE and DoD Hotline.

Personal Security Concerns

When you completed your original Questionnaire for National Security Positions (QNSP) or Electronic Questionnaire for Investigative Process (e-QIP) and when a renewal of your clearance was requested, you were made aware of your responsibility to report certain personal information. Those reporting responsibilities are ongoing.

The following information is to be reported no later than two (2) working days after the event, and three (3) days by written notification, unless noted otherwise, to the UC Research Security Office.

- **Arrests**

Report all arrests, including charges that are dismissed.

- **Criminal Charges**

Report all criminal charges including felony, misdemeanor, public and petty offenses as defined in the statutes of any state.

- **Detention by Law Enforcement**

Report any detention by federal, state or other law enforcement authority for violation of law.

- **Traffic Violations**

Report any traffic violations for which you receive a fine of $300 or more unless the traffic violation is alcohol or drug related. **Any traffic violation that is alcohol or drug related must be reported regardless of the fine.**

- **Ongoing Contact with Foreign Nationals**

Report employment, business & personal related associations with any foreign national or employees/representatives of a foreign-owned interest.

Personal Security Concerns Continued

The following information is to be reported no later than two (2) working days after the event, and three (3) days by written notification, unless noted otherwise, to the UC Research Security Office.

- **Hospitalization**

Report hospitalization for treatment of mental illness or other mental condition; treatment for alcohol or drug abuse; any condition that may cause a significant impairment in judgment or reliability.

- **Bankruptcy**

Report any personal or business-related bankruptcy.

- **Wage Garnishment**

Report all wage garnishments including, but not limited to, divorce, delinquent debts or child Support.

- **Name Changes**

Report all legal name changes.

- **Change in Citizenship**

If you are a U.S. citizen who changes citizenship or acquires dual citizenship, you must report this change to Personnel Security.

- **Change in Marital Status**

Report marriage or cohabitation *within 45 days* of the event.

Foreign Travel

Clearance holders must provide notification of personal and business travel outside the United States at least 45 days prior to travel to UC Research Security Office. The following table is a guideline regarding travel requirements:

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 counter-intelligence officer	Required only if suspicious contact made
University-funded with DOE contract funds	Any foreign country	Required[3]	To Research Security Office 45 days prior to travel[4]	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 Ernest Orlando Lawrence Berkeley National Laboratory.

[2]See http://labs.ucop.edu/security/sensitivecountries.html 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.

[4]UC employees assigned to work at the Ernest Orlando Lawrence Berkeley National Laboratory should contact Elijah Walker to obtain the required DOE foreign travel approvals.

Incidents of Security Concern (IOSC)

An Incident of Security Concern (IOSC) occurs any time there is a potential or actual compromise of classified or Unclassified Controlled Information (UCI) or when a security rule is violated. Incidents of Security Concern are actions, inactions or events that have occurred that:

- Pose threats to national security interests and/or critical DOE or DoD assets.
- Create potentially serious or dangerous security situations.
- Potentially endanger the health and safety of the workforce or public (excluding safety related items).
- Degrade the effectiveness of the safeguards and security program.
- Adversely impact the ability of organizations to protect DOE or DoD safeguards and security interests.

If you observe, find or have knowledge of or information regarding an IOSC, you must immediately report it to the UC Research Security Office.

Leaves of Absence

A security clearance must be terminated if the clearance holder is on leave of absence or extended leave from the position for which the clearance is required and will not require access for at least ***90 calendar days*** as a result of being on leave. (This includes leave for sabbatical, travel, medical reasons, and extended annual/sick leave, not involving official U.S. Government business.)

This 90-day period may be adjusted at the discretion of the DOE Personnel Security Office (PSO) or the Director, Office of Security for DOE.

When a clearance holder goes on a leave of absence as described above, they are required to:

- Complete the Leave of Absence Extension Request Form.
- Sign the DOE F 5631.29, Security Termination Statement.
- Surrender his or her Federal Credential.

Terminations

When a Regent's term ends or an employee's relationship with the University is ended through retirement, resignation or termination, they are required to:

- Complete a security termination briefing.
- Sign a DOE F 5631.29, *Security Termination Statement.*
- Sign the SF-312, *Classified Information Non-disclosure Agreement*.
- Surrender his or her Federal Credential.

UC-sponsored Federal Credentials are issued by the Lawrence Livermore National Laboratory (LLNL) Badge Office. It is the Regent's or employee's responsibility to ensure that the badge is returned to the UC Research Security office (who will forward the badge to LLNL) when it is no longer needed, no longer valid, or if it becomes damaged.

Failure to return your government issued badge upon request or termination will result in the badge being treated as stolen government property and reported to the appropriate federal law enforcement authorities.

Waste, Fraud and Abuse Hotline

Waste, fraud and abuse, whether a crime is involved or not, must be reported to the UC Research Security Office, the UC, or the Inspector General. These reports can be made anonymously.

Information of whom and how to make a report to UC is available online at:

http://www.universityofcalifornia.edu/hotline.

Reports to DOE and DoD are to be made directly to the Inspector General of each agency through their hotline listed below:

DOE Hotline: Inspector General of the Department of Energy
(800) 541-1625
E-mail: IGhotline@hq.doe.gov

DoD Hotline: Inspector General of the Department of Defense
(800) 424-9098
E-mail: hotline@dodig.mil

Section 3:
Classified Matter Protection and Control

Objectives

After successfully completing this section, you will be able to:

- Recall how to secure classified matter.
- Identify responsibilities regarding the use of Unclassified Controlled Information (UCI).
- Identify the categories of UCI.
- Be aware of the penalties regarding the unauthorized disclosure of classified information.

Securing and Handling Classified Matter

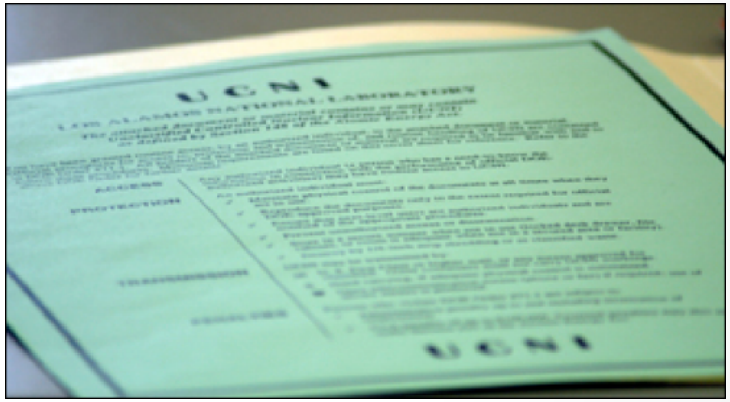
Classified matter can be in many forms; it can be held, it can be seen, and it can be heard. It is the responsibility of each employee who has access to any form of classified matter to ensure that it is handled properly. The following requirements are used to ensure the protection and security of classified matter:

- Conduct classified work and discussions only in approved areas (Those areas do not generally exist at UCOP or the Lawrence Berkeley National Laboratory. Contact the UC Research Security Office for information about what areas are approved for discussion of classified matters).
- Protect classified matter from individuals without a need to know even if they the have required security clearance.
- Never leave classified matter unattended.
- Conduct telephone conversations involving classified information only over approved telecommunication devices. Those devices are specialized and you should contact the UC Research Security Office about how and where you can conduct a telephone conversation involving classified information.
- Never remove classified matter from approved storage facilities to private residences or other unapproved places such as hotel rooms.

Unclassified Controlled Information (UCI)

Even unclassified documents may contain sensitive information.

Unclassified Controlled Information (UCI) is broadly defined as federal government-owned information that may be exempt from public release either by statute, or under the federal Freedom of Information Act and for which disclosure, loss, misuse, alteration or destruction would adversely affect national security or government interests. UCI, formerly known as Sensitive Unclassified Information (SUI), is unclassified information requiring control with respect to handling, storage, and distribution.



Categories of UCI

The following designations are types of unclassified controlled information that are frequently encountered:

- Official Use Only (OUO).
- Personally Identifiable Information (PII).
- Unclassified Controlled Nuclear Information (UCNI).

Official Use Only (OUO): Federal government-owned information that is unclassified yet exempt from release to the public under the federal Freedom of Information Act. This information consists of sensitive administrative, proprietary, or personal information that warrants protection from unauthorized disclosure.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, such as his/her name, social security number, date of birth, place of birth, mother's maiden name, biometric data, etc. This information, unlike other forms of UCI, need not be federal government-owned. University-owned records that contain this information are also considered to be PII.

Unclassified Controlled Nuclear Information (UCNI): UCNI is certain unclassified federal government-owned information that has been determined to fall under the purview of the following Atomic Energy Commission (AEC) programs:

- Nuclear material production.
- Safeguards and Security.
- Nuclear weapons design.

(Unclassified Controlled Nuclear Information is protected by law because it can provide an adversary with easy access to information that has the potential to damage our government and therefore must be protected at all times.)

Controlling Access to UCI

A person granted routine access to Unclassified Controlled Information (UCI) must have **a need to know** the specific information in the performance of official or contractual duties. Because UCI is unclassified, a security clearance is not required; however, recipients must be advised of the protection requirements.

UCI must be protected at all times from unauthorized disclosure. UCI must be stored in a locked room or locked receptacle with the key controlled only by individuals meeting the need-to-know criterion.

Classified Information in the Public Domain

Information that is considered classified by the US government, may, on occasion, appear in the public domain, in print, or in broadcast media reports. However, the appearance of such information in open sources does not automatically make it unclassified.

In accordance with DOE's "No Comment Policy", as a cleared employee, you cannot comment on any classified information that appears in the public domain. This includes articles in newspapers or magazines, books, speeches, etc. The fact that classified information is in the public domain is itself classified; therefore, you cannot comment on the accuracy, technical merit, or classification status of such classified information.

If you are not sure about the classification status, you should avoid comment. Also, remember that just because classified information has appeared in the public domain does not mean that the information is declassified.

Unauthorized Disclosure of Classified Information

Unauthorized disclosure is the communication or other provision of classified information to an unauthorized person. Using classified information in a manner detrimental to the United States or to the benefit of a foreign country also constitutes unauthorized disclosure. Knowing and willful unauthorized disclosure is a crime. Employees can cause an inadvertent unauthorized disclosure—communicating classified or sensitive unclassified information without meaning to do so. Using a basic knowledge of security processes and procedures can prevent inadvertent disclosures.

Civil Penalties for Classified Information Security Violations

- Title 19, U.S.C., Section 798, "Disclosure of Classified Information", has a maximum penalty for authorized disclosure of no more than $250,000 or imprisonment not more than 10 years, or both.

- Section 234B of the Atomic Energy Act of 1954 authorizes the Department of Energy to take enforcement action, under Title 10 CFR Part 824, "Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations," against DOE contractors that violate DOE classified information security requirements.

Section 4:
Counterintelligence, Threat Awareness and OPSEC

Objectives

After successfully completing this section, you will be able to:

- Understand the role of Counterintelligence.
- Identify possible collection methodologies.

What is Counterintelligence (CI)?

Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities.

The best way to counter threats is to know the targets, know your adversaries, know how to protect and report information and always report any suspicious information activity or attempts to obtain information.

Threats can come from many places: foreign governments, competitors, and even trusted insiders (e.g. coworker).

Possible Collection Methodologies

Foreign governments are in the information business and employ a variety of means to obtain it:

Request for information – direct and indirect requests for information (e.g. e-mails, phone calls, conversations). A simple request can net a piece of information helpful in uncovering a larger set of facts.

Solicitation or Marketing of Services – foreign-owned companies seek business relationships to enable them to gain access to sensitive or classified information, technologies, or projects.

Public Venues – conferences, conventions, symposiums and trade shows offer opportunities for adversaries to gain access to information and experts in dual-use and sensitive technologies.

Official Foreign Visitors and Exploration of Joint Research – foreign government organizations, including intelligence and security services, consistently target and collect information through official contacts and visits.

Foreign Targeting of U.S. Travelers Overseas – foreign collectors target U.S. travelers overseas. Collection methods include everything from eliciting information during seemingly innocuous conversations, to eavesdropping on private telephone conversations, to downloading information from laptops and other digital storage devices

To counter these threats, it is important to report these occurrences. Any vulnerability, no matter how seemingly inconsequential, should be reported to the UC Research Security Office as soon as possible.

Operations Security (OPSEC)

"Operations Security" (OPSEC) is an systematic process used to mitigate vulnerabilities and protect information, generally unclassified, about you or your organization. OPSEC does not replace other security disciplines - it supplements them.

OPSEC is not only for Military or Government entities. Individuals and companies are realizing more and more the importance of protecting trade secrets, personal security and/or intentions.

The principles of OPSEC are based on asking five questions:

1. What information do you want to protect?

2. Who wants your information?

3. How is your information vulnerable?

4. What is the risk for your information?

5. How can you protect your information?

OPSEC:
How Can I Do My Part?

- Use passwords to access your computers.
- Guard against phone calls seeking personal and sensitive information.
- Watch possible inadvertent ways in which we release information.
- Think about the sensitivity of the information you handle.
- Be careful of what you throw out in the trash.
- Watch what you post on the Internet use groups and chat rooms.
- Do not place files containing sensitive information on your laptop - it may get stolen.
- Practice "Need to Know".

Remember

You are responsible for meeting all security requirements. It is an important responsibility and should not be taken lightly. **EVERY** individual is held accountable for his or her actions, and each individual must choose to follow the established security rules. Be certain you understand these rules and make the right choices each and every day.

Resources

Acronyms

CI	Counterintelligence
CUI	Controlled Unclassified Information
DOE	Department of Energy
DoD	Department of Defense
e-QIP	Electronic Questionnaire for Investigative Process
IOSC	Incidents of Security Concern
LANL	Los Alamos National Laboratory
LLNL	Lawrence Livermore National Laboratory
NISPOM	National Industrial Security Program Operating Manual
OPSEC	Operations Security
OUO	Official Use Only
PII	Personally Identifiable Information
PSO	Personnel Security Office
QNSP	Questionnaire for National Security Positions
UCI	Unclassified Controlled Information
UCNI	Unclassified Controlled Nuclear Information

Resources Continued

Websites

Berkley Lab Travel Website
http://travel.lbl.gov/

Department of Energy
http://energy.gov/

DOE Sensitive Countries Listing
http://labs.ucop.edu/security/sensitivecountries.html

Department of State Travel Website
http://travel.state.gov

Defense Security Service
http://www.dss.mil

Laboratory Management
http://labs.ucop.edu

National Nuclear Security Administration
http://www.nnsa.energy.gov

UC Research Security Office
http://labs.ucop.edu/security/index.html

Security Regulations (not all inclusive):

- Executive Order 12958, as amended - Classified National Security Information
- Executive Order 12968 –Access to Classified Information
- Director of Central Intelligence Directive No 6/4
- DoD 5200.2-R, DoD Personnel Security Program
- DoDD 5205.2, DoD Operations Security (OPSEC) Program
- DoD 5200.8-R, DoD Physical Security Program
- DoDD 2000.12, DoD Antiterrorism (AT) Program
- Homeland Security Presidential Directive (HSPD-12)
- DOE O 472.2, Personnel Security
- DOE O 475.1, Counterintelligence Program
- DOE M 470.4-1 Section K, Safeguards and Security Awareness Program

2012 Annual Refresher Briefing Acknowledgment

After reading the Annual Security briefing, please sign the acknowledgment below and forward to the University's Assistant Facility Security Officer, Brandi Marotta, by email to Brandi.Marotta@ucop.edu or by fax to (510) 839-3831.

I have read and understand the Annual Security Briefing.

NAME (in print):_____ SIGNATURE:_____

DATE:_____