University of California
2010 Annual Refresher Briefing

Protecting Our America~Your National Laboratories

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

University of California
2010 Annual Refresher Briefing

TABLE OF CONTENTS

Introduction

I. Overview of the Security Classification System

II. Reporting Requirements

III. Reinvestigations

IV. Foreign Travel

V. What is OPSEC?

VI. Resources

Acknowledgment of Briefing

INTRODUCTION

Welcome to the University of California's 2010 Annual Security Refresher Briefing. The purpose of the Annual Refresher briefing is to reinforce the initial security briefing information that you received when your clearance was granted, and to inform you of any significant changes in security procedures/requirements promulgated by the Government. As the federal security regulations require, the annual security refresher briefing addresses site-specific issues and selectively reinforces other information. This year's briefing focus is **reporting requirements** for all clearance holders.

The University sponsors clearances for three different groups:

- non-employee Regents (as key management personnel required to be cleared under federal requirements due to their potential impact on security policies and practices);
- University employees and consultants involved in oversight of University classified contracts or joint ventures; and
- 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.

Due Date Response

Please acknowledge your 2010 refresher briefing by October 30, 2010.

Ronald A. Nelson
Facilities Security Officer (FSO)
Research Security Office
and
Executive Director, Contracts & Administration
Laboratory Management Office
University California Office of the President

I. OVERVIEW OF THE SECURITY CLASSIFICATION SYSTEM

The University of California performs 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.

THE SECURITY CLASSIFICATION SYSTEM

A security clearance (access authorization) means that you are eligible to be granted access to classified information or material at the level of CONFIDENTIAL, SECRET, or TOP SECRET, based on the extent of your background investigation and based on your NEED TO KNOW, as related to your assigned oversight responsibilities for the national security Laboratories for which the University has parent oversight responsibilities (i.e., the Los Alamos and Lawrence Livermore National Laboratories).

DEFINITIONS OF CLASSIFIED INFORMATION

For a better understanding of your involvement with classified information when you visit the Los Alamos or Lawrence Livermore National Laboratory or any other facility with classified information, 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.

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 *in addition to* possessing personal security clearance for that level of classified 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.

II. REPORTING REQUIREMENTS

This year's area of emphasis for the annual security refresher briefings is reporting requirements. This section deals with –

- Why reporting requirements exist
- What are the reporting requirements
- How and to whom to report

As further described below, there are generally three categories of reporting: (1) personal facts, (2) security incidents, and (3) changes in need for access to classified information.

PERSONAL FACTS

The application for a security clearance, Questionnaire for National Security Positions (QNSP), involves providing extraordinary access to the government to private, personal information in exchange for access to national security information. The more sensitive the information to which you gain access, the more intrusive is the government inquiry into your life and circumstances.

In the course of applying for a personal security clearance you give the government (1) information that uniquely identifies you to the exclusion of all others, and (2) information about your –

- relationships, family and personal connections
- physical and mental health history
- work history
- education
- residences
- finances
- civil disputes
- police involvement
- travel outside of the United States
- security clearances
- political activities
- use of information technology systems

The reporting requirement of personal facts after the granting of a personal security clearance is essentially a "living" QNSP. That is, when certain key events occur that change the information originally collected by the government in the initial background investigation or periodic reinvestigation, those events are to be reported. The table titled *Personnel Reporting Requirements* at http://labs.ucop.edu/security/secforms.html identifies those key events.

Why is this specific information required to be reported? The answer is based on our nation's long experience with individuals who have demonstrated themselves to be untrustworthy or disloyal. This experience has been distilled into thirteen (13) adjudicative criteria that the government uses when determining whether an individual should have or continue to have a personal security clearance:

- allegiance to the United States

- foreign influence
- foreign preference
- sexual behavior
- personal conduct
- financial considerations
- alcohol consumption
- drug involvement
- emotional, mental, and personality disorders
- criminal conduct
- security violations
- outside activities
- misuse of information technology systems

U.S. citizens are presumed to be loyal to our country. Accordingly, the purpose of the investigation is not to prove an individual is trustworthy and loyal, but to look, instead, for the existence of specific conditions that raise a security concern, and then consider any mitigation of that concern.

When the criteria are examined in detail[1] many relate in some way to the three principal motivations for compromise of national secrets: (1) sex, (2) money, and (3) ideology. That these motivations continue to be highly relevant are illustrated as follows:

Sex

Sexual attraction is a powerful tool in spy craft. Since Biblical times stories abound with seduction being used to obtain information either willingly or as the price for keeping embarrassing facts private. In the spy business this is known as a "honey trap."

In 2008, an aide to then-British Prime Minister Gordon Brown fell victim to a honey trap. The unidentified aide was approached by a woman in a Shanghai disco while enjoying a little down time on a trade mission with the Prime Minister. The woman went back with the aide to his hotel room. The next morning he discovered his BlackBerry was missing.

The London Times reported in January 2010[2] that the British Government has sent out a restricted warning to businesses, banks and financial institutions to be wary of honey traps:

> *China has occasionally attempted sexual entrapment to target senior British political figures*.
>
> *The report says the practice has now extended to commercial espionage*.

[1] The complete text of the adjudicative criteria is found at 32 Code of Federal Regulations, Part 147 ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION, Subpart A.

[2] http://www.timesonline.co.uk/tol/news/uk/crime/article7009749.ece

"Chinese intelligence services have also been known to exploit vulnerabilities such as sexual relationships and illegal activities to pressurise individuals to co-operate with them."

While the issuing of the report is news, the technique is not. Phillip Knightly recently authored "The History of the Honey Trap"[3] for *Foreign Policy Magazine*. In it he details several famous cases, but here are three than you may not have heard much about:

- An Israeli technician, Mordechai Vanunu, took the story of the Israeli Atomic bomb to the *London Sunday Times* in 1986. Vanunu was supposed to keep out of sight in a London safe house while the *Times* checked out his story. But, instead, he was seduced by an American-born Israeli agent and lured to Rome. There he was kidnapped by Mossad and returned to Israel for trial and incarceration.
- Jeremy Wolfenden, was the *London Daily Telegraph's* correspondent in Moscow in the 1960s. It become known by the KGB that Wolfenden was gay. He was then seduced by a man under orders by the KGB who took photographs and threatened to expose Wolfenden's sexual orientation if he did not cooperate with the KGB. Wolfenden revealed his predicament to the British Secret Intelligence Service. Their response was to put him, not entirely voluntarily, to work as a double agent.
- In the 1950s an East German Stasi officer, Markus Wolf, recognized that with the shortage of men in post-war West Germany, more single women had entered into government service. He developed a corps of "Romeo spies" where he recruited many handsome East German men to cross the border and seduce and compromise these single women. One of the successfully targeted women was able to become a secretary in the office of West German Chancellor Helmut Schmidt. Another woman became a spy in NATO and reported on the deployment of nuclear weapons.

Money

In February of this year we all got to see on "60 Minutes" 51 year old Gregg W. Bergersen agreeing on video to provide secret defense information to a Chinese government agent. Bergersen was sentenced in July 2008 to a little over four years in prison for selling information on planned U.S. sales of weapons and military technology to Taiwan for the next five years. The sale was to a Taiwanese-born Louisiana businessman, Tai Kuo. Kuo, although a naturalized U.S. citizen, represented to Bergersen that he was an agent for the Taiwanese government. But Kuo was in fact acting on behest of the People's Republic of China.

Bergersen was director of the C^4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) program for the Defense Security Cooperation Agency. Kuo compromised Bergersen with gifts, Las Vegas gambling trips and promises of future employment after his retirement from the Pentagon.

And Bergersen was not Kuo's only target. James W. Fondren Jr., 62, a retired Air Force lieutenant colonel who later worked at the Pentagon as a civilian, was convicted in September 2009 of giving Kuo classified information through roughly 30 "opinion papers" he sold to Kuo between 1998 and 2007. He sold these papers for between $350 and $1500 apiece. Eight of the

[3] http://www.foreignpolicy.com/articles/2010/03/12/the_history_of_the_honey_trap?page=full

papers contained classified information. The papers dealt primarily with U.S.-Taiwanese military relations. Like Bergersen, Fondren believed Kuo to be working for Taiwan; he was apparently unaware that he was the object of a "false flag" operation. In January Fondren was sentenced to three years in prison.

Ideology

73 year old Walter Kendall Myers and his 72 year old second-wife, Gwendolyn, were sentenced in July to life without parole and 81 months, respectively. What did they do? They passed secrets to Cuba for nearly 30 years. Why did they do it? They were dedicated to what they saw as Fidel Castro's socialist nirvana in the Caribbean.

Kendall Myers was an academic who in his 1972 PhD dissertation, *A Rationale for Appeasement*, argued that Neville Chamberlain had sensibly seen the national socialist (Nazi) government of Germany as "Britain's natural ally" in the 1930s and recognized "the threat that the United States posed to the Empire." How and why he developed such an antipathy toward the United States is particularly puzzling given that he was a great-grandson of Alexander Graham Bell, inventor of the telephone, and grandson of Gilbert Grosvenor, editor of the *National Geographic* for 55 years. He also had the benefit of a first-rate education at Brown and Johns Hopkins Universities and material wealth and position in society.

But nevertheless, Kendall was identified as a potential asset by the Cuban Intelligence Service in 1977. He was invited to Cuba and was guided in that trip by a Cuban agent. The Cuban accounts of victimhood by the United States deeply impressed him. Apparently thereafter his wife Gwen became an ally and they commenced to secretly act on behalf of the Cuban government.

Kendall sought out teaching and analyst positions within the State Department that would give him access to information of value to Cuba. He even developed a certain level of celebrity within the State Department. In 1995, Kendall and Gwen were honored, secretly, at a dinner with Fidel Castro that included other honors for their service to the communist dictatorship.

> *"The trouble with this country, there's just too many North Americans," Kendall told an undercover FBI agent…who was posing as a Cuban intelligence officer in April 2009. The downside of lifting the Cuban travel embargo, Kendall quipped, was that "believe me, those North Americans, you don't want them."*

Within days after their arrest in June 2009, Fidel Castro released the following statement:

> *"I can't help but admire their disinterested and courageous conduct on behalf of Cuba. Those who in one form or another have helped to protect the Cuban people from the terrorist plans and assassination plots organized by various U.S. administrations have done so at the initiative of their own conscience and are deserving, in my judgment, of all the honors in the world."*

A fascinating account of the Myers and their journey into betrayal can be found in Tony Harden's account for Washingtonian magazine[4] from which some of the statements in this

[4] http://www.washingtonian.com/print/articles/6/171/13751.html

summary were drawn. If you apply the 13 adjudicative criteria to many of the events in their lives set forth in that account, alarm bells should have been ringing.

These stories demonstrate the continuing necessity of the government to monitor personal facts relating to clearance holders. The table titled *Personnel Reporting Requirements* at http://labs.ucop.edu/security/secforms.html identifies those personal facts that must be reported as they occur.

SECURITY INCIDENTS

It's not hard to remember that known violations of controls over classified information must be reported. These violations include the unauthorized release of, failure to properly secure, or failure to properly mark, classified documents. But "security incidents" also includes *unsuccessful* attempts to get an individual with personal security clearance to improperly disclose classified information[5]. A lack of success may be either because the individual declined to disclose the requested information or because he/she did not have access to the information. Nevertheless, the attempt must be reported.

These general rules apply to all personal security clearance holders. But individuals who routinely access classified information also need to also familiarize themselves with special security requirements relevant to their activities. For more information please visit http://labs.ucop.edu/security/index.html.

CHANGE IN ACCESS NEEDS

Personal security clearance is based on a current need to access classified information. A person requires access not only if he/she is routinely reviewing or looking at classified documents, but if his/her job responsibilities require access to classified information when certain contingencies arise that must be addressed without the delay entailed in obtaining personal security clearance.

Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Title III of that Act adopted certain reforms – automated systems, unitary investigation authority, reciprocity, and adjudication time standards – designed to make personal clearance granting faster and more uniform across the government. In exchange for more timely clearance processing, contractors are expected to terminate or downgrade clearances whenever the need for access ends or the level of classification of information to which access is required is reduced. Therefore the preferred situation is that personal security clearances be terminated and reinstated or downgraded and upgraded, whenever it is known that the current need for access to classified information or a level of classified will be different for a substantial period of time.

Although there is no specific guidance as to what a substantial period of time may be, the Research Security Office uses the standards established by DOE Albuquerque Service Center for individuals on leave of absence: No action must be taken to terminate or downgrade a clearance if the change in access requirements is known to persist for less than six months. An action must

---

[5] Contacts by foreign nationals, not related by blood or marriage, are a "personal fact" to be reported where "a relationship that is enduring, involves substantial sharing of personal information and/or the formation of emotional bonds" is established, even if there is no apparent attempt to obtain classified information.

be taken to terminate or downgrade a clearance if the change in access requirements is expected to persist for a year or more. An action should be taken promptly to terminate or downgrade a clearance if the change in access requirement is of an indeterminate length. Where the length is time is determinable but falls between six months and a year, decisions will be made on a case-by-case basis and may require notice to DOE.

The University must terminate a clearance whenever an individual with personal security clearance leaves our employ and/or there is no contractual relationship with him/her. However, if the individual is immediately entering into a contractual relationship with another entity for which personal security clearance is required, the University and that entity can coordinate to avoid the complete termination of the personal security clearance.

For all of the reasons stated above, a personal clearance holder or supervisor (if applicable) must notify the Research Security Office when changes in need for access to classified information occur or termination of employment or contract is expected. The table titled *Personnel Reporting Requirements* at http://labs.ucop.edu/security/index.html summarizes that reporting requirement.

UC, DOE, AND DOD HOTLINES

In addition to reporting requirements of one's own conduct or circumstances, 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 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

III. REINVESTIGATIONS

Clearance holders are periodically reinvestigated for trustworthiness and loyalty. Individuals with DOE Q and/or DoD Top Secret clearances have a single scope background investigation (SSBI) conducted every five years; individuals with DOE L and/or DoD Secret or Confidential clearance have a National Agency Check with Local Check (NACLC) conducted every ten years. Reinvestigations for individuals holding both DOE and DoD clearances are conducted by DOE as the cognizant agency over the University's facility clearance.

Starting in 2009, the U.S. Department of Energy National Nuclear Security Administration Service Center at Albuquerque, NM initiates and processes all reinvestigations of UC individuals with DOE Access Authorizations "L" and "Q." As a result, the clearance holder and not the Research Security Office gets notice of the reinvestigation and copies of the associated documents. Upon your receipt of an email message, you will have 30 days to complete the information for your clearance update. An example of the email can be seen at http://labs.ucop.edu/security/secforms.html. As part of the package, the Research Security Office *does* execute and submit to the Service Center an updated AL F 470.1 "Clearance Action Request". Contact the University's Research Security Officer for assistance with clarification or if you cannot locate your previously completed SF-86 Security Questionnaire.

IV. 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[6]	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[7]	Not Required	To Research Security Office prior to travel	Discretionary – may be requested by DOE counterintelligence officer	Required only if suspicious contact made
University-funded with DOE contract funds	Any foreign country	Required[8]	To Research Security Office 60 days prior to travel[9]	Mandatory	Mandatory

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".

[6] 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.
[7] See http://labs.ucop.edu/security/sensitivecountries.html for a list of sensitive countries.
[8] 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.
[9] UC employees assigned to work at the Earnest Orland Lawrence Berkeley National Laboratory contact Elijah Walker to obtain required DOE foreign travel approvals.

V. OPSEC

We all have access from time to time to unclassified information that also requires some level of protection. Examples include social security numbers, personal information, credit card and bank accounts, trade secrets, intellectual property, and possibly information restricted from export out of the U.S. The University, as an academic enterprise, values openness and equal access to knowledge and minimizes the circumstances in which information is created or possessed that cannot be freely disseminated. But as the listing above shows, there *is* information even for employees in an academic enterprise that either must be or should be protected.

In a commercial and military setting the term Operations Security or OPSEC is used to refer to the obligations and techniques used to protect unclassified commercially or militarily valuable information from a competitor or foe. Below is a standard OPSEC briefing used in those contexts. As you read through it, mentally translate some of the terms into your own professional and personal life; think about the harms that can occur to the University, you or others when information that should be protected is acquired by someone who would exploit it to the detriment of the University, you or others:

WHAT IS OPSEC?

Operations security (OPSEC) is an analytic process used to deny an adversary information, generally unclassified information, concerning friendly intentions and capabilities by identifying, controlling, and protecting indicators associated with planning processes or operations. OPSEC does not replace other security disciplines - it supplements them.

OPSEC is simply denying an adversary information that could harm you or benefit them. Another form of OPSEC, although not as widely accepted, is the intentional misinformation of an adversary, designed to protect your true secrets.

OPSEC is a process, but it is also a mindset. By educating oneself on OPSEC risks and methodologies, protecting sensitive information becomes second nature.

OPSEC is not only for Military or Government entities. More individuals and Corporations are realizing the importance of protecting trade secrets, personal security and intentions. Whatever the organization and purpose, OPSEC can, and will, increase the overall security posture.

WHY OPSEC?

We are in a world increasingly dependent on information. In this world, pieces of information (internet postings, work schedules, phone directories and more) may be assembled in order to form the "big picture" of an organization or operation.

Your adversaries practice OPSEC to varying degrees, and it would be unwise to discount the capabilities of your adversary. Your adversary will constantly probe your organization, so the importance of a solid understanding of OPSEC cannot be understated.

WHAT ARE OPSEC INDICATORS?

An indicator is a "piece of the puzzle". In other words, an indicator is any piece of information that can be exploited to gain further information, or be combined with other indicators to build a more complete profile of your operations.

For example, an OPSEC indicator could be when you go to work, what you do at work, large group movements or financial transactions such as life insurance appointments. Before releasing information, consider the potential value to your adversaries.

WHAT ARE THE CAPIBILITIES OF YOUR ADVERSARY?

The unfortunate fact is that you don't know. Your adversary may have internal spies, skilled photographers or any other manner of resources at their disposal. You may never be able to determine the full capability of your adversary, so you can only protect your information on your end.

VI. RESOURCES

WEBSITES

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

Department of Energy
http://doe.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

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

2010 ANNUAL REFRESHER BRIEFING ACKNOWLEDGMENT

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

I have read and understand the Annual Security Briefing.

NAME (in print):_____ SIGNATURE:_____

DATE:_____