UNIVERSITY *of* CALIFORNIA

>> 2008 Annual Refresher Briefing

PROTECTING OUR AMERICA: YOUR NATIONAL LABORATORIES

Argonne National Laboratory • Brookhaven National Laboratory • Continuous Electron Beam Accelerator Facility • Fermi National Accelerator Laboratory • Hanford Technical Library • Idaho National Engineering Laboratory • Lawrence Berkeley National Laboratory • Lawrence Livermore National Laboratory • Los Alamos National Laboratory • National Renewable Energy Laboratory • Oak Ridge National Laboratory • Pacific Northwest National Laboratory • Sandia National Laboratories • Stanford Linear Accelerator Center

2008
Security Refresher
Briefing

NOTICE TO SECURITY CLEARANCE HOLDERS

Introduction

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 significant changes in security procedures/requirements promulgated by the Government. Two significant changes recently announced are (1) adoption of a standardized federal credential by October 27, 2008 replacing your DOE badge as a form of identification and access authorization; and (2) adoption of a new Standard Form 86 (revised July 2008) replacing the current September 2005 version. In response, we have developed UCOP Interim Guidelines for implementing DOE's new re-badging requirements. Included in the briefing for your review is a link to the revised SF 86 that the University must begin using for new applicants, reinvestigations and reinstatements, beginning January 1, 2009. We have also provided you with a brief overview reminder of the Security Classification System. Finally, we have briefly summarized OPSEC principles and their importance in the security world, as well as in your everyday lives.

Your Responsibility Remember – Your security responsibilities are ongoing. We encourage you to carefully review the material in this briefing to better understand various security policies applicable to your University-sponsored security clearance.

Due Date Response

Please acknowledge your 2008 refresher briefing by January 15, 2009.

Willie C. Archie   R L Van

Willie Archie
Facilities Security Officer (FSO)
UC Laboratory Management

Robert Van Ness
UC Associate VP Operations & Adm.
UC Laboratory Management

Contents

REQUIREMENT FOR STANDARDIZED FEDERAL CREDENTIAL PERSONAL IDENTITY VERIFICATION

BACKGROUND

On August 27, 2004, the White House announced Homeland Security Presidential Directive 12 (HSPD-12) that addressed the problem of inconsistent and potentially insecure forms of identification that were used to access Federal buildings and information systems. The goals of the Directive were to increase security, reduce identity fraud and increase efficiencies within the government.

To implement the requirements of HSPD-12 related to the secure and reliable identification of Department of Energy (DOE) Federal and contractor employees, DOE issued Directive DOE N 206, effective November 22, 2005. HSPD-12 requirements are being instituted incrementally and require the Facility Security Officer (FSO) to visually inspect 2 picture IDs of an applicant for a security clearance, (i.e., drivers' license, passport, etc.) in addition to making copies of those documents for the applicants security file. The FSO must certify to DOE that the Personal Identity Verification (PIV) process has occurred. Currently, the DOE security badge has been determined to be the Department's Federal Agency identity credential in compliance with HSPD-12. "PIV'ed" individuals are expected to receive the compliant DOE security badge, sometime during the course of calendar year 2009.

NEW CREDENTIAL REQUIREMENT TO REPLACE DOE BADGES

As part of the incremental implementation of HSPD-12, effective October 27, 2008 all federal facilities, including the national laboratories, are required to adopt a standardized federal credential that will replace DOE badges as a form of identification and access authorization. All UC-sponsored clearance holders will be required to have a federal credential that will replace their current LLNL-issued badge.

CREDENTIAL SPECIFICATIONS

All credentials will have start and end dates, and will be valid for 5 years. (For the purpose of this section "credentials" = "badges.") These new credentials (badges) will be issued to all University cleared personnel who require them.

SUMMARY: NEW BADGE (CREDENTIAL) **Objectives** Upon completing this module, you will be able to identify: • The process for obtaining a replacement badge (a.k.a. credential). • The different types of credentials.	
In Brief- All federal facilities, including LLNL and LANL, are required to adopt a standardized federal credential for implementation in order to replace current DOE badges. LLNL does not have a specific completion date at this time. The federal credential will replace your DOE badge as a form of identification and access authorization.	
WHO… **…will receive the new federal credential?**	Every UCOP-Cleared employee, contractor, and consultant who has a DOE badge will be required to have a federal credential that will replace their current badge. All credentials will have start and end dates, and will be valid for 5 years.
Continued	

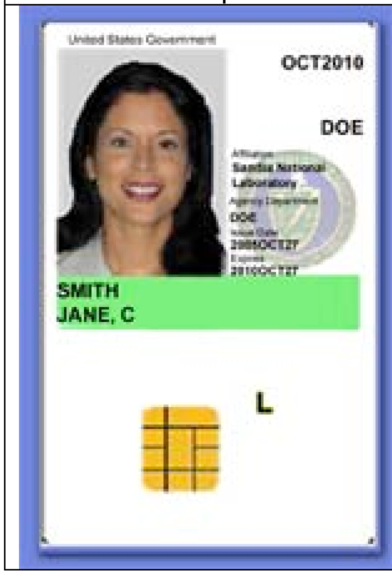
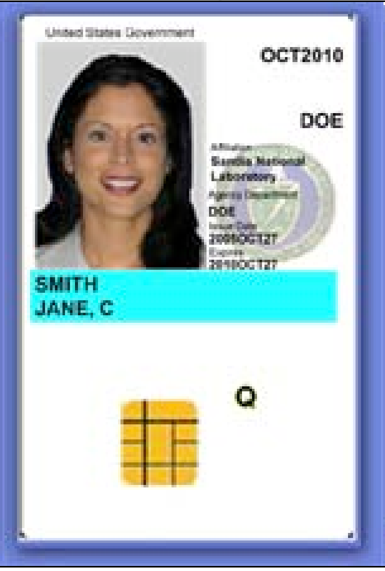
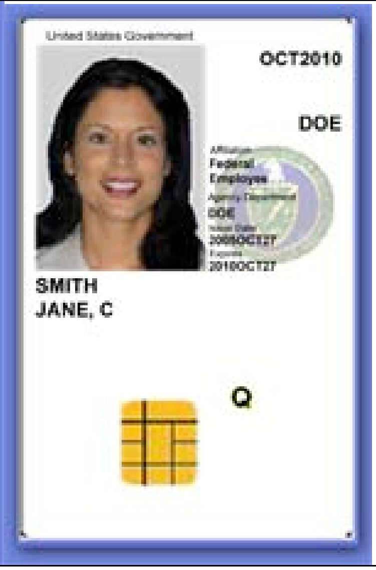
WHY… **do I need a federal credential?**	Homeland Security Presidential Directive 12 (HSPD-12), issued August 27, 2004, established a goal of eliminating the wide variations in the quality and security among forms of identification used to gain access to secure federal facilities where there is a potential for terrorist attacks. Subsequently, the National Institute of Standards and Technology (NIST) developed a standard for a “smart card” credential that will include secure unique information about each credential holder. The security features that NIST established for the federal credential are: • Based on sound criteria to verify individual’s identity. • Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation. • Used for rapid electronic verification of personal identity. • Applicable to all government organizations and contractors. • Used to grant physical access to federally controlled facilities. • Used to grant logical (cyber) access to federally controlled information systems. This feature will be implemented at the Labs at a later date. • Not applicable to identification associated with national security systems. • Implemented in a manner that protects individual privacy.
Continued	

WHAT… **…makes the credential "smart"?**	Each credential contains the following components: • Integrated circuit chip (ICC) that stores 64KB of data that includes: o Four Public Key Infrastructure (PKI) digital certificates (Personal Identity Verification [PIV] authentication, card authentication, digital signature, and encryption). o Two interoperable fingerprint templates. o Digital photo. o Cardholder Unique Identifier (CHUID), including organization affiliation, agency affiliation, department affiliation, and expiration date. • Magnetic stripe.

WHAT…
…will the credential look like?

Your federal credential will also look different from your current DOE badge. **It will not have color-coding to indicate clearance level.** Instead, colored stripes will indicate the type of individual, as follows:

- Federal Contractor (includes UC employees, contractors, and consultants) – green stripe.
- Foreign national – blue stripe.
- Federal employee – white (essentially no stripe because the background is also white).
- Additionally, first responders will have a separate red stripe on the bottom of their credentials.

Federal Contractor* Green stripe	Foreign National Blue stripe	Federal Employee White (no stripe)
 United States Government OCT2010 DOE Affiliation Sandia National Laboratory Agency Department DOE Issue Date 2008OCT27 Expires 2010OCT27 SMITH JANE, C L	 United States Government OCT2010 DOE Affiliation Sandia National Laboratory Agency Department DOE Issue Date 2008OCT27 Expires 2010OCT27 SMITH JANE, C Q	 United States Government OCT2010 DOE Affiliation Federal Employee Agency Department DOE Issue Date 2008OCT27 Expires 2010OCT27 SMITH JANE, C Q

*Employees, contractors and consultants.

WHEN… **…will I receive my new credential?** 	Lawrence Livermore National Laboratory (LLNL) is planning to host two credentialing centers for the Livermore area. Other credentialing centers will be established throughout the United States, including Southern Nevada, where one or more will be located in the Las Vegas area. When the credentialing centers are operational University of California Key Management Personnel and UCOP-cleared employees will be enrolled first, followed by cleared UCOP contractors and consultants. When it is your turn to receive a federal credential: 1. You will be notified by e-mail to schedule an appointment online at a specified credentialing center, most likely the Lawrence Livermore National Laboratory. 2. During your first visit, you will be required to present two forms of identification (one of which must be a government-issued ID), and you will be fingerprinted. 3. Approximately 3 weeks later, you will be notified to return to the credentialing center to pick up your credential. 4. During the return visit, you will be required to show one form of photo ID, and you will have a new set of digital fingerprints compared to index fingerprints taken at the time of enrollment.

End of Section Questions

1. All cleared federal employees and contractors will be required to have a federal credential.

   a) True
   b) False

2. The goal for issuing the new federal credential is to eliminate wide variations in the quality and security of forms of identification used to gain access to secure federal facilities where there is potential for________.

   a) Protests
   b) Military units
   c) Terrorist attacks
   d) Layered security

3. A cleared foreign national badge will be:

   a) White with red stripe
   b) White with blue stripe
   c) White with green stripe
   d) Layered security

Answers to end of section questions

1. a) True
2. c) Terrorist attacks
3. b) White with blue stripe

0VERVIEW OF THE SECURITY CLASSIFICATION SYSTEMS

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 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., LLNL and LANL).

DEFINITIONS OF CLASSIFIED INFORMATION

For a better understanding of your involvement with classified information when you visit the weapons 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 II.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 Laboratories – Frequently the Laboratory Management Office within the UC Office of the President assists with arranging visits and briefings at the 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).

0PERATIONS SECURITY PRINCIPLES

BACKGROUND

There exists in the world of security various disciplines to minimize risks caused by adversaries. One of these disciplines includes Operations Security (OPSEC). The OPSEC Process not only has national security applications to thwart the plans of an adversary, but many of the principles can also be applied to our individual personal life and safety environments.

The standard OPSEC principles are:

- Identify Critical Information
- Analyze the Threats
- Analyze Vulnerabilities
- Assess Risk
- Apply Countermeasures

FURTHER EXPLANATION OF OPSEC PRINCIPLES

Identify Critical Information – What are we trying to protect? Is it our home when we are away on vacation or the credit cards we have in our wallets or purses?

Analyze Threats – Who wants or needs our critical information? Who is our adversary (not necessarily an enemy)? Is it the drug user that needs money for obtaining illegal drugs or criminal seeking to steal our wealth? What Critical Information do they already know about us? Credit card information we left in our trash containers, newspapers piled up in front of our home when we departed for vacation? Inappropriate or inadvertent disclosure on web pages of our credit card information?

Analyze Vulnerabilities – How will the Critical Information collected on us be used? What if known may be used to our disadvantage? Is the Vulnerability Low (potential for exploitation is negligible, or is potential high) from a High Vulnerability assessment? Internet charges with our credit card account number, break-in of our homes to steal valuables because they know we are away? Break-in of our home while our family is present?

Assess Risk – Risk can be quantified by the simple formula of Consequence x Vulnerability x Threat = Risk. What is the risk to our lives or to our family if a measure is implemented? If implemented but not effective because we thwarted the operation of canceling our credit card, or if a neighbor called the police when they discovered a stranger in our back yard?

Apply Security Countermeasures – What solutions can we employ to reduce risks to an acceptable level, whether by eliminating vulnerabilities, disrupting the effective collection of information, or by preventing the adversary from accurately interpreting the data?

Some Simple Countermeasures

Identify Your Critical Information

Memorize Passwords / PINS – Don't Record Them on Anything

Send files Electronically vice Hard Copy

Buy Cross-Cut Shredders to destroy unwanted credit cards and personal checks from financial institutions

Protect/Destroy: Old Credit Cards, Thumb Drives, Flash Drives, Memory Cards, Cell Phones, CDs/DVDs

Stop your newspapers at least 2 days before you depart on vacation; inform a trusted neighbor of your plans and ask that they watch over your home.

Links to further OPSEC references:

http://www.opsecprofessionals.org/origin.html

http://www.defendamerica.mil/articles/a021202b.html

REVISED SF86 QUESTIONNAIRE
FOR NATIONAL SECURITY POSITIONS

BACKGROUND

The Office of Personnel Management (OPM) has announced the revision and testing of the July 2008 updated version of the current September 1995 version of the Standard Form 86 "Questionnaire for National Security Positions" (SF86). The old SF86 form will not be accepted after January 1, 2009 target date. The General Services Administration (GSA) indicates the old form is currently out of stock.

New applicants, along with clearance holders undergoing reinvestigations of their current security clearances, will use the new SF86 form beginning January 1, 2009 (current target date). At this time, until OPM has fully tested the new form all current UC clearance holders and new applicants will continue to use the old SF86 form while processing their applications.

HIGHLIGHTS OF NEW REQUIREMENTS

There are many changes in the new version of the SF86.

Click on the following link "SF86 Revised" to view the entire content of the new SF86 Questionnaire for National Security Positions. The UC Security Website will have the current SF86 version in effect and will update the website when the new SF86 is implemented. Refer to website at http://labs.ucop.edu/security/index.html click on "Other Security Forms."

Highlights of some of the changes to the SF86 form are:

1. Many of the sections have been renumbered and the information required is more specific, such as home phone and home email. If you have a passport, you will be required to provide the number.

2. On page 16 you are asked if you have failed to pay Federal, state or other taxes, or to file a tax return required by law or ordinance.

3. The Medical Release Form has been revised to allow your Physician to attest to your mental capacity or judgment to protect classified information.

ACKNOWLEDGEMENT

Please email willie.archie@ucop.edu to acknowledge that you have read this version of the University of California 2008 Security Refresher Briefing. Include the following statement in the body of your message:

I acknowledge receipt of the University of California 2008 Security Refresher Briefing in compliance with U.S. Department of Energy and U.S. Department of Defense security requirements.

It is important to include your name after the above statement. We will be contacting you if your email statement is not received by January 15, 2009.

Thank you.

Willie Archie