

Unauthorized Disclosure Awareness Training - 35045

Training Requirements

Due to a number of recent security incidents involving potential unauthorized disclosure of classified information, this training was developed to inform you of your security responsibilities, specifically to help reduce the number and severity of these incidents. This training is for all individuals at the Laboratory who have the potential to electronically post or transmit classified information. Your Responsible Line Manager has established a process to ensure a qualified Authorized Derivative Classifier, other than the author, reviews related material before it is posted or transmitted.

Integrated Safeguards and Security Management

This (ISSM) Integrated Safeguards and Security Management approach of defining the scope, analyzing the risk, developing controls, performing the work, and ensuring performance should be incorporated within your organization's Integrated Work Documentation or IWDs.

We cannot put classified information at risk!

Activity Risk Categorization

The Director's Instruction does NOT require that ALL posted information be reviewed by an Authorized Derivative Classifier, or ADC, prior to transmission, rather, only those that represent a potential risk of unauthorized disclosure. The activity risk categorization process will assist you with classification recognition.

For each activity, project, or research area you work with, your Responsible Line Manager, using ADCs as Subject matter experts, categorize the risk of generating classified information that could be disclosed.

There are three risk categories.

- Unrestricted
- Conditional
- Restricted

If the risk category of your activity is Restricted, then you must have the information reviewed by an ADC, other than the original author, who is knowledgeable in the pertinent subject matter. Transmission of information in the Conditional category without ADC review requires that you have undergone classification awareness training as specified by your line manager. Without successful completion of such training, this category also requires that you have an ADC review.

When in doubt, always check with an ADC before distributing any questionable information.

You can find a list of [ADCs online](#)

What to Protect?

Classified information is defined as any information that requires protection against unauthorized disclosure to avoid damage to national security.

We more commonly use the term classified matter, which is an all-encompassing term to include documents, parts, and/or media, which may contain or reveal classified information.

How to Protect?

To help protect our classified matter we must make sure two requirements are met. First, your clearance level must be commensurate with the classified document level and secondly, you must have a need to know. Need to know is a determination made by the authorized holder of that classified matter that an individual with the proper clearance level requires access to that information in order to perform or assist in tasks that are essential to a project or job they have been assigned.

Always remember that all work involving classified information must be conducted only in approved security areas. Classified matter must not be left unattended at any time. When not in your physical control it must be stored in an approved GSA safe, vault, or vault-type room.

Classification Levels and Categories

The classification level and category tells us the extent of protection the classified matter needs. The classification level represents how much our national security could be damaged if the information were to be released.

We have three levels of classified information: Top Secret, Secret, and Confidential.

- Top Secret information can be expected to cause exceptionally grave damage to our national security if the unauthorized disclosure happened to take place.
- Secret can be expected to cause serious damage, and
- Confidential can be expected to cause damage.

The classification category describes the type of information.

We also have three categories.

- Restricted Data,
- Formerly Restricted Data, and
- National Security Information.

Restricted Data deals with information that is related to the design, manufacturing, and testing of our nuclear weapons. Formerly Restricted Data is information that pertains to the military utilization of our atomic weapons, and National Security Information is all other information that does not contain nuclear weapons related information.

If your work may involve classified information, it is your responsibility to understand which information is classified and to properly protect such information.

Unclassified Information

When releasing unclassified information, you must always obtain an official Los Alamos publication identification number for all work presented outside of the Laboratory. A LA-UR (" or Unlimited Release") is assigned to documents and other materials that could be released to the public. You must submit an abstract or summary for all technical talks presented outside of the Laboratory on unclassified subjects. LA-URs can be anything from a one-paragraph abstract to a 1,000-page report being sent to a reading room for public availability. The LA-UR submission process can be found online.

If you have any questions, contact the Classification Group, S-7, Publications Release Team at **667-5013**.

Unclassified Controlled Information

Unclassified Controlled Information or UCI refers to information in which the disclosure, loss, misuse, alteration, or destruction could adversely affect national security. There are several different types of UCI. Unclassified Controlled Nuclear Information (or UCNI) and Official Use Only (or OUO) are the most common.

Unclassified Controlled Nuclear Information

UCNI is sensitive government information that is controlled even though it is not classified. You do not have to hold a clearance to view UCNI but you must have a need to know. Security measures taken to protect UCNI transmissions must deter access by unauthorized individuals and restrict public release. UCNI must be protected by an approved encryption method when transmitted over public switched broadcast communications paths such as the Internet. UCNI may be transmitted by email without encryption if the sender and receiver are behind the LANL firewall, however, it is recommended that you encrypt UCNI even within the firewall.

Official Use Only Information

OUO is applied to information that is unclassified yet exempt from release to the public under the Freedom of Information Act. In general, this information consists of sensitive administrative or personal information that warrants protection from unauthorized disclosure. Markings are required for documents containing OUO information.

Documents with OUO information must be marked: on the bottom of the front page or cover page and on each interior page or each interior page containing OUO information, with the legend; OFFICIAL USE ONLY.

For more information about Unclassified Controlled Information, see the Security website "Protecting Information" or contact the Security Help Desk at 665-2002.

Who Can Help?

Your line manager and your organization's ADCs can assist you with assigning a risk category and classifying your information correctly.

Regardless of the work you do, all of the material you produce that is intended for public release, such as professional journal articles, conference proceedings or posters, open web postings, and formal or informal reports, must be submitted for review and release by S-7 before leaving the Laboratory. If you have any questions, contact your ADC, S-7 or the Security Help Desk.

The bottom line is to ensure you have your work reviewed for classification BEFORE you transmit or share technical information which may be classified.

Do Not Risk It!

BRIEFING ACKNOWLEDGEMENT

I certify I have read the Los Alamos National Laboratory's Security & Safeguards Unauthorized Disclosure Awareness Briefing. The contents of this briefing will be reviewed and updated annually. If you print this briefing for usage throughout the year you are responsible for assuring you have the most current version. Credit will not be provided if the most current briefing content was not read. The last update of this briefing was May 31, 2005.

OPTION 1 - Online Credit Submission

If you have a Cryptocard with administrative access you can submit for credit using the "Receive Credit" button and your training record will be updated within the hour. If you do not have a Cryptocard, you must submit for credit to the S Division Registrar. Crediting of your training record will be completed within three days or sooner.

Receive Credit

OPTION 2 - Fax or Mail

Please allow up to 5 working days before credit will appear in Employee Development System (EDS) database if faxing or mailing this page.

Z # _____

Name – printed _____

Signature _____

Date _____

Phone Number _____

Or Please fax to:
(505) 665-8984

Or mail to:
S-Division Registrar
PO Box 1663
Mail Stop K560
Los Alamos, NM 87545