LA-UR 97-5197

nos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

TITLE: **A GUIDE TO UNCLASSIFIED SENSITIVE INFORMATION PROTECTION**

AUTHOR(S): Stephen C. Donahue

SUBMITTED TO: External Distribution

Los Alamos

Los Alamos National Laboratory
Los Alamos New Mexico 87545

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

A Guide to Unclassified Sensitive Information Protection

CIC (RI)-001.000

November 14, 1996

Division Security Office
Computing, Information, and Communications Division
Los Alamos National Laboratory
Los Alamos, New Mexico

Abstract

This document is a reference guide for CIC-Division employees who lead or participate in projects that use and/or produce unclassified sensitive information. It is intended for use on a case-by-case basis to develop project-specific sensitive information handling procedures and standards. It contains criteria for identifying sensitive information and determining levels of sensitivity, and describes cost-effective measures for protecting various levels of sensitive information. The goal of this document is to help establish good business practices that benefit both the Laboratory and its customers. Division personnel are encouraged to apply these guidelines.

Unclassified Sensitive Information Protection Guide
Table of Contents

Unclassified Sensitive Information Protection Guide
Table of Contents

Unclassified Sensitive Information Protection Guide

Sensitive Information Protection Summary

This Summary provides a condensed list of recommended protection mechanisms for CIC-Division projects handling unclassified information. The tasks and protection mechanisms abbreviated in this Summary are expanded in the subsequent documentation.

I. General Protection Requirements

I.1 All Projects

Project management are strongly encouraged to ensure that:

a. diligent efforts are made to identify any sensitive information (Section 3);

b. each user registers on-line, and determines the sensitivity level of the information that s/he will be processing;

c. project personnel receive training about their computer security and other related security responsibilities as established by the Laboratory Computer Protection Program Manager (CPPM) and the CIC Division Security Officer; and

d. project personnel and management formally acknowledge acceptance of their security responsibilities.

I.2 Projects With Unclassified Sensitive Information

In addition, if any project information is deemed sensitive, project management are required to ensure that:

e. a determination is made of the information's sensitivity level (Section 4).[1]

Furthermore, project management are strongly encouraged to:

f. appoint a project Security Administrator (Section 2).

[1] This step is essential for completion of the affected Protection Plans, and will aid considerably in the selection of appropriate protection measures (Section II).

II. Protection Recommendations

II.1 Low Risk Information (Non-Sensitive)

The Low Risk (Section 4.1.1) sensitivity level involves unclassified non-sensitive information. This is information whose disclosure, loss of integrity, or unavailability, would result in minor or no adverse impact on the information owner's interests. However, because of the cost expended to generate or regenerate this information, projects handling such information should:

1. on a regularly scheduled basis, use virus detection programs, where available, on all systems; and

2. establish procedures to protect against malicious codes (viruses, worms, Trojan horses, etc.).[2]

II.2 Medium Risk Information

The Medium Risk (Section 4.1.2) sensitivity level involves sensitive information whose disclosure, loss of integrity, or unavailability would have an adverse impact on the information owner's interests. Projects handing such information should follow all Low Risk protection measures, plus (to the level deemed appropriate for the information involved):

3. screen all project personnel (Section 6.1);

4. establish and practice need-to-know procedures for all project personnel with access to sensitive information (Section 6.2);

5. follow the protection practices detailed in Section 6.3 (such as passwords, screen savers, and access controls);

6. follow good information handing practices (Section 6.4);

7. select equipment and connectivity appropriate to the technical needs of the project and the sensitivity of the information (Section 6.5);

8. control access by unauthorized visitors (Section 6.6);

9. follow good off-site practices (Section 6.7);

10. prepare and keep current a Project Protection Agreement with the information owner (Section 7.1);

[2] Such as might be acquired with untested freeware downloaded from the Internet or from unrestricted movement of media such as diskettes and tapes.

11. maintain a current list of Project Protection Mechanisms (Section 7.2);

12. determine project criteria for need-to-know, and maintain a current list of those to whom it has been conferred; and

13. encourage all project personnel to participate in ongoing training so that they have up-to-date knowledge of those factors that affect their responsibilities in this area.

II.3 High Risk Information

The High Risk (Section 4.1.3) sensitivity level involves sensitive information whose protection is based on contract, legislative, directive, or regulatory requirements that include the penalty of law for violations. Projects handing such information should follow all Low and Medium Risk protection measures, plus should employ the following additional protections:

14. use protected (e.g.., encrypted) communication when transmitting off-site, as described in Section 6.4.8;

15. use session controls on multi-user systems (Section 6.3, issue 8); and

16. segregate project-specific information from other projects (Section 6.4.1).

II.4 Extreme Risk Information

The Extreme Risk (Section 4.1.4) sensitivity level involves sensitive information whose protection is life- or mission-critical. Projects handing such information should follow all Low, Medium, and High Risk protection measures, plus should:

17. formalize disaster recovery and contingency planning (Section 6.8).

Unclassified Sensitive Information Protection Guide

1. INTRODUCTION

1.1 Purpose

Certain unclassified information requires some degree of protection from disclosure to unauthorized persons, from unauthorized alteration, and from loss. This is *sensitive information.* All users of Los Alamos National Laboratory (LANL) computer systems are required to make a determination of the sensitivity of all information they create, access, and use. If any of their information is sensitive, they have an obligation to handle that information as required by Federal and State legislation, DOE orders, and Laboratory policy.

This document is a reference guide for CIC-Division employees who lead or participate in projects that utilize unclassified sensitive information. It provides options for identifying and protecting such information in reasonable and cost effective ways. It is for use on a case-by-case basis; and contains criteria for identifying sensitive information and for determining levels of sensitivity, and measures for protecting various levels of sensitive information. The goal of this document is to help establish sound business practice in the area of information handling that benefit both the Laboratory and its customers. Division personnel are strongly encouraged to apply these guidelines. However, except where explicitly stated, they are not mandatory.

The information in this guide is a compilation of information derived from the many references listed in Section 8.

1.2 Overview

Negligent handling of sensitive information by LANL employees can have severe repercussions. It can undermine the integrity and credibility of the Laboratory, cause the loss of valued customers, and lead to costly litigation involving civil and criminal penalties for both the Laboratory *and* individual employees. Furthermore, incidents involving mishandling of sensitive information can negatively impact the ability of the Laboratory to attract new customers, endangering the viability of the Laboratory. Given this shared liability, it behooves *every* LANL employee to assume responsibility for protecting sensitive information. Each may do his or her part by ensuring that each project handling sensitive information meets state and federal laws governing sensitive information, DOE requirements for the handling of sensitive information, the expectations of the customer, and the dictates of common sense.

1.2.1 Who Is Responsible

Responsibility for unclassified sensitive information protection rests with both the *information owner* and the *information stewards.* The information owner legally possesses the information. Information stewards, those with legitimate access to the information, have responsibility for properly managing the information under their control, this responsibility being derived from the information owner. In our lexicon, the information owner is usually a project customer, i.e., the buyer of a service or product. This customer may be either internal or external to LANL. Information stewards are project personnel, usually LANL employees. Each of these roles has its inherent obligations and duties.

1.2.1.1 The Customer

The customer has a responsibility to adequately identify and (where appropriate) label information that the customer regards as sensitive. In other words, the obligation is on the customer to specifically identify sensitive information.

1.2.1.2 Project Personnel

Our customers, whether they be internal or external to the Laboratory, generally count on project personnel to satisfy their technical goals. They trust that this technical expertise will deliver the desired product. However, they may not consider the problem of sensitive information protection, especially the technical issues that arise in today's complicated computing environment. It is therefore the responsibility of project personnel and their accountable management to address the issue of sensitive information protection, whether or not the project's customer has raised or shown concern for the issue. When necessary, project personnel should take it upon themselves to educate the customer of the potential hazards posed to electronic information in the chosen computing environment, and the methods by which that information may be protected.

1.2.2 Legal Position

The Laboratory is subject to a variety of laws, regulations, and orders. It is of course governed by Federal statutes and regulations. Through its connection to the University of California, it is governed by California statutes. Finally, it should follow DOE Orders. Section 8 provides a list of pertinent DOE orders, Federal legislation and regulations, and LANL documentation.

1.3 Basic Requirements

1.3.1 Security Administration

Accountable managers should ensure that each project for which they are responsible is reviewed for information sensitivity. They have the responsibility and authority to identify and formally appoint a security administrator to each project that handles sensitive information. Section 2 elaborates Security Administration responsibilities and requirements.

1.3.2 Identify and Rank Sensitive Information

Each project should determine the sensitivity of all information that the project uses, stores, creates, and/or distributes throughout the project. Each type of information handled on the project should be assigned a sensitivity level. Section 3 defines sensitive information and gives guidance on how to identify it. Section 4 guides the assignment of sensitivity levels to project information.

1.3.3 Perform a Risk Assessment

There are often conflicts between the goals of ideal information protection, the cost and inconvenience of that protection, and the information access and technical requirements of the project. In addition, the owners of sensitive information have great latitude in deciding how to protect their sensitive information. Therefore, every project should perform a risk assessment to provide project personnel and the customer with the information necessary to establish appropriate protections for sensitive information. Section 5 defines the risk assessment process and provides guidance in performing such an assessment.

1.3.4 Establish Protection Mechanisms

Project personnel should establish appropriate protection mechanisms for all project information. Particular protection mechanisms are based on the level of information sensitivity assigned according to this guide (Section 4). Section 6 describes common vulnerabilities, details available protection mechanisms that mitigate the vulnerability, and makes recommendations for use. The summary at the beginning of this document lists the protection mechanisms recommended for each level of information sensitivity.

1.3.5 Document

Both the levels of information sensitivity and all selected protection mechanisms are agreed to in negotiations with the information owner. All such agreements should be documented and signed by the information owner and all project personnel. By signing the agreement, all parties agree to abide by the established protection mechanisms. Section 7 details documentation requirements.

1.3.6 Revisit

Information sensitivity invariably changes over time. For example, after a press release or the assignment of a patent, a customer's proprietary information may no longer require the same level of information protection as it did before those significant events. Therefore, it is essential that the sensitivity determination process be repeated at significant intervals throughout the life of the project.

2. SECURITY ADMINISTRATION

Each project that handles sensitive information should have an individual who is responsible for security administration on that project. This individual will have the responsibility and should have the authority to ensure that project personnel adhere to the requirements covered in this guide. The Security Administrator may be the Group's Organizational Computer Security Representative (OCSR), the Project Leader, or any other appropriately trained individual.

At a minimum, the project Security Administrator should:

- have a working knowledge of computer security issues, particularly those involving sensitive information;
- know what protection mechanisms (physical, administrative, and electronic) are available at LANL (e.g., the Open ICN, vaults, exclusion areas, etc.) for handling sensitive information;
- if required, provide an interface to the Industrial Partnership Office (IPO);
- have an adequate technical background in computing and networking; and
- be familiar with those portions of the LANL Administrative Manual and Office Procedures Manual that provide LANL policy regarding sensitive information;

and be capable of:

- working with FSS Division personnel to interpret the LANL Computer Security Policies, DOE Orders, Federal statutes and regulations, and other laws to which LANL is subject;
- working with Laboratory Legal Counsel (LC) personnel to resolve business and legal issues that arise regarding sensitive information; and
- working with project personnel to understand the needs of the project with respect to sensitive information.

3. IDENTIFY SENSITIVE INFORMATION

3.1 Who Decides?

In some cases, the issue of sensitivity has already been decided by State and Federal legislation, by DOE regulation, or by LANL policy. In the remaining cases, the determination of what information is sensitive, how sensitive, and who may access it, is made by the owner of the information. In these cases sensitivity determinations are based on the owner's judgment of the impact of loss, misuse, corruption, unavailability, and/or unauthorized disclosure of the information.

3.2 What is Sensitive Information?

In brief, sensitive information is information that, if lost or compromised, would:

- negatively affect the owner of the information to an unacceptable level;
- jeopardize the ability of a system to continue processing; and/or
- require substantial resources to recreate.

3.2.1 To Business

In the corporate world, examples of sensitive information that should be kept confidential include:

- Banking fund transfers
- Oil resource data
- Stock futures strategies
- Medical research data
- Airline reservation information

Sensitive information whose integrity should be ensured includes:

- Electronic funds transfers

3.2.2 To the US Government

According to the US Government, sensitive information is "information the disclosure, alteration, loss, or destruction of which could adversely affect national security or other federal government issues." Examples of information sensitive to the US Government include:

- Productivity statistics (National Institute of Standards and Technology)

- Currency production and transfer information (Department of the Treasury)

- Embassy personnel information (Department of State)

- Primary interest rate changes (Federal Reserve)

What makes this information sensitive is that its theft or modification could potentially disrupt the nation's economy or compromise its employees. Similarly, the breach of individual health and financial records maintained by such agencies as the Social Security Administration (SSA), the Federal Bureau of Investigation (FBI), the Internal Revenue Service (IRS), and the Census Bureau could have severe legal and personal repercussions.

3.2.3 To LANL

LANL regards the following as examples of sensitive information:

- *Life or Mission Critical Unclassified Information* is plain text or machine-encoded unclassified data that, as determined by competent authority (e.g., information owners), has high importance related to accomplishing a LANL mission and requires a degree of protection because unnecessary delays in processing could adversely affect the ability of an owner organization, site, or the Laboratory to accomplish such missions. For example, the information managed by the LANL Alarm system for security and fire protection purposes is considered mission critical.

- *Limited Access Information* is privileged information that should not be disclosed to the public except through proper channels. Examples include information on employees, budgets, finances, security, incidents, legal issues, and life critical safety critical issues (LANL AM 708, OPM-1-1).

- *Privacy Act Information* is information of a private nature on individuals. For example, information on personnel, drug test results, test scores, payroll, radiation exposure records, and accident reports (LANL AM 708, OPM-1-1).

- *Controlled Scientific and Technical Information (Proprietary)* is information entrusted to LANL by private sources or developed by LANL at private expense, or research and development information of an experimental nature (LANL AM 721, DOE Order 1430.1D, DOE Order 1700.1)

- *Unclassified Controlled Nuclear Information (UCNI)* is certain unclassified government information prohibited from unauthorized dissemination under section 148 of the Atomic Energy Act (As Amended) For example, nuclear defense programs, and nuclear production facilities designs (DOE Order 5630.3, DOE Order 5635.4)

Additional information is available in Los Alamos' *Unclassified Sensitive Information Identification and Protection Manual* [22].

3.3 Questions to Ask

The following questions are intended to assist in determining whether project information is sensitive, and who makes the determination:

1. Who owns the information? Where does the information originate?

2. Who is the current information steward?

3. Who are the users of that information?

4. Is the information covered by State or Federal legislation?

5. Is the information covered by DOE or other regulation?

6. What are the impacts of loss of confidentiality, loss of integrity, loss of availability, destruction, or unauthorized distribution of the information?

7. What is the criticality of the information? Is its unauthorized disclosure critical? Is loss of its integrity critical? Is its availability critical?

8. What events could alter the information's sensitivity?

9. Do you have any doubts at all about the sensitivity of the information? If so, ask your project's Security Administrator, the information owner, your Project Leader, your OCSR, or the appropriate Group in FSS Division (see Section 10).

4. RANK SENSITIVE INFORMATION

4.1 Levels of Sensitive Information

Information that is determined to be sensitive should be protected at a level commensurate with its sensitivity. A critical step is the assessment and assignment of information sensitivity levels. Establishing different levels of sensitivity allows project personnel and customers to determine what protections are appropriate for the information, since rules for physical and electronic protection vary according to the impacts of loss, corruption, misuse, unavailability, or unauthorized disclosure of that information. Sensitivity level assignment is sometimes determined by law, regulation, or established Laboratory policy. Where not thus covered, level assignment may be done by the information owner, with the assistance of LANL personnel, or by LANL personnel with the approval of the information owner. The important point is that all responsible parties accept the determination of sensitivity levels for their information.

4.1.1 Low Risk Information

The level assignment *Low Risk* is given to unclassified information that requires no protection against disclosure. It either has no requirement for integrity or loss of integrity will only have a minimally adverse affect on the interests of the owner of the information. Its unavailability will have no, or little, adverse affect on the interests of the owner of the information.

4.1.2 Medium Risk Information

The level assignment *Medium Risk* is given to unclassified information designated as sensitive by the information owner. This is information whose premature or incomplete disclosure, loss of integrity, or unavailability could result in a significant negative customer impact, and whose compromise would result in loss of customer confidence and would have an adverse affect on Laboratory interests. The owner has complete control over sensitivity determinations of this information. Examples of such information include (but are not limited to):

- Project Status Information - such as the success or failure of specific research or development efforts.

- Intellectual Property - such as ideas, inventions, expressions, unique names, business methods, techniques, and formulas.

- Trade Secrets - include commercially valuable information that gives the owner a competitive business advantage. It can include technology, sales information, customer lists, pricing policies and practices, marketing strategies and plans, new products, requirements and specifications, product performance data, budgets, business plans, production details, etc.

- Protected CRADA Information - technical information that is developed through a CRADA and could be commercially valuable.
- Protected WFO Information - technical information that is developed through a WFO agreement and could be commercially valuable.
- Protected Cost-Shared Information - commercially valuable information that is produced in cost-shared agreements other than CRADAs and WFO agreements with nonfederal parties.
- LANL Protected Information - LANL-developed information that LANL considers valuable and that could be used commercially.
- State Department Protected Information - Sensitive but Unclassified (SBU) or Limited Official Use (LOU).
- DOD Protected Information - For Official Use Only (FOUO).
- Department of Energy Official Use Only (OUO). Information that may be exempt from pubic release under the Freedom of Information Act (FOIA) of 1967. These may include internal Laboratory personnel rules and practices, and proprietary information obtained from companies working with the Laboratory.
- Ancillary project information such as records of project existence and goals, project membership lists, and meeting schedules.
- Nondisclosure agreements - legal compacts that private industry requires to be in place before its representatives will discuss sensitive information.

4.1.3 High Risk Information

The level assignment *High Risk* is applied to unclassified information whose premature or incomplete disclosure, loss of integrity, or unavailability will adversely affect Laboratory interests. It is information whose protection is mandated by policy, regulation, directive, contract, legislation, or agreements between the DOE, its contractors, and other entities such as commercial organizations and foreign governments. Even the information owner is required to protect this information in a prescribed manner. Such information includes that covered by the California Information Practices Act (CIPA), the Privacy Act of 1974, the Atomic Energy Act of 1954, The Arms Export Control Act, and The Export Administration Act of 1979. This category includes (but is not limited to):

- Personal information such as financial and medical records, employment history, and performance evaluations.

- Information critical to the safety of the US nuclear power capability.
- Unclassified Controlled Nuclear Information (UCNI). Information that could reasonably be expected to have a significant adverse affect on public health and safety by a) significantly increasing the likelihood of illegal production of nuclear weapons or b) significantly increasing the likelihood of theft, diversion, or sabotage of nuclear materials.
- Export Controlled Information (ECI). This is technical information that requires a license to export, beyond the unrestricted General License.
- DOE "Applied Technology" is information limited to specific domestic recipients, to retain foreign trade value.
- Naval Nuclear Propulsion Information (NNPI). Unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair, of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated nuclear support facilities.

4.1.4 Extreme Risk Information

The level assignment *Extreme Risk* is applied to unclassified information that is designated mission- or life-critical. It is information whose premature or incomplete disclosure, loss of integrity, or lack of availability will adversely affect DOE or national interests. Such information includes, but is not limited to:

- Department of Energy Mission Critical Information.
- The information managed by the LANL Alarm system for security and fire protection purposes.

4.2 Questions to Ask

The following questions are intended to assist in determining the information level:

1. Is the information covered by legislation, regulation, or policy?
2. Is the information critical to the mission of the Laboratory?
3. Might the information be export controlled?
4. Does the information contain personal data?
5. Would the loss of confidentiality, integrity, or availability of the information result in a significant negative impact to the owner? to the Laboratory? to the DOE? to the national interest?

6. Do you have any doubts at all about the sensitivity level of the information? If so, ask your project's Security Administrator, the information owner, your Project Leader, your OCSR, or the appropriate Group in FSS Division (see Section 10).

5. RISK ASSESSMENT

5.1 What is a Risk Assessment?

Risk assessment is a process used to estimate potential losses that may result from system vulnerabilities, and the quantify the damage that may result from certain threats. The ultimate goal of a risk assessment is to help select cost-effective protection measures that will reduce risk to an acceptable level. An adequate risk assessment may be an informal process, but should include an examination of:

- the project's information needs;
- the cost of losing and/or regenerating or recovering the information;
- the current information vulnerabilities, and how likely they are to be exploited in different ways; and
- legal and regulatory protections for the information.

In other words, a risk assessment is performed to determine what information protections the project warrants and can support.

Generally, the information owner decides what risks are acceptable, and thus what protections will be used. However, when the information is subject to legal or regulatory protections, these should be considered when deciding protections. *A customer's decision not to protect sensitive information as required by law or regulation may not absolve Los Alamos employees from legal liability.*

Different projects have different security concerns and will, therefore, have to set their priorities and policies accordingly. Project personnel will have to thoroughly understand the needs of the project operational environment and users, and define project protection measures accordingly. Not every protection described in this guide is appropriate to every project. Furthermore, the more elaborate the security measures get, the more expensive and restrictive they become, and the more difficult it may be to complete the project.

To set up appropriate protection measures, project personnel need to understand potential risks and the cost of preventing, or recovering from, the damage associated with those risks. Remember, risk can only be reduced, it can never be eliminated. No matter how secure a computer, it's protections can be breached given sufficient resources, time, and money.

Start the risk assessment with a well thought out set of priorities. Decide what has to be protected and what the cost might be to prevent any losses versus the cost of recovering from those losses. Then decide what protection measures are appropriate for a prioritized list of most critical needs. Don't just include computers; also include backup tapes, network connections, workstations, and documentation. They are all part of the system and represent opportunities for potential loss. Finally, remember that people are often the weakest link.

5.2 Questions to Ask

The following questions are intended to assist in a risk assessment:

1. What information do you have and how important is it?

2. How vulnerable is the information under the current protection mechanisms?

3. What is the cost of losing or compromising the information?

4. What is the cost of protecting the information?

5. What are the project information access and availability needs? Is remote access or only local access required? Is immediate availability required, or is delayed availability sufficient?

6. What are the information transmission requirements and mechanisms?

7. What are the clearance levels of project personnel and customer personnel? Are any of the project personnel foreign nationals, particularly from sensitive countries? What personnel screening has been performed?

8. Is there a backup strategy in place? Is one needed?

9. What protection mechanisms are in place or are needed?

10. What resources can the project and/or the customer bring to bear on the establishment of protection mechanisms? What is the budget for protecting the information?

6. PROTECTION MECHANISMS

6.1 Personnel Screening

Basic personnel screening is performed for all Laboratory personnel before employment. The Project Leader and the Information Owner have the authority to require more in-depth personnel screening as they deem necessary to ensure the protection of sensitive information.

6.1.1 Types of Employment

The various types of employment assignments at the Laboratory include:

- Regular full-time and part-time University of California employees
- Post-Doctoral Appointees
- Graduate Research Assistants
- Undergraduate and High School Students
- Subcontractors. These include those with contracts to supply people as-needed, those with major services contracts such as Johnson Controls International and Protection Technology Los Alamos, and those with individual task contracts such as architectural engineering firms.

6.1.2 Typical Employment Screening

The personnel screening for regular University of California employees ranges from the basic pre-employment check to full background investigations, depending on the level of clearance the employee has. Post-Doctoral Appointee and Graduate Research Assistant credentials are thoroughly reviewed by their respective Laboratory hosts and their associated University officials. Undergraduate and high school students are screened by their school administrators before being recommended to the Laboratory for employment.

The personnel screening for subcontractors varies from minimal references checks to full background investigations, depending on the level of clearance the employee has. All subcontractor employees have a pre-employment screening as required by Laboratory contracts.

6.1.3 Additional Screening

Project Leaders and Information Owners may require additional screening of project personnel based on the sensitivity of the information. With the acknowledgment and permission of each affected individual, the Project Leader may initiate an extended background check that includes financial, legal, medical, and/or psychological investigations. The Human Resources (HR) Division undertakes these background checks and, to avoid any conflict of interest, ensures that they are performed by qualified independent contractors.

6.2 Need-to-Know

Sensitive information should be shared only with those individuals with a clear need-to-know. Need-to-know limits a person to only the information needed for the person to perform a particular function. Unless the need-to-know has been established, assume that someone does not have it. Every project should establish (or adopt previously existing) mechanism(s) by which need-to-know is conferred, and to whom, and should specify the minimum criteria that should be met by anyone who is granted the need-to-know. Be aware of the information transmission mechanisms in use by the project to ensure that sensitive project information does not fall into the hands of anyone without a need-to-know.

6.3 Core Protections

Project personnel should adhere to the following security protections when processing sensitive information on any computer system:

1. Label the system "Sensitive Unclassified" when processing sensitive information.

2. Ensure that a computer's monitor screen cannot be viewed by unauthorized individuals.

3. Do not leave sensitive removable disks in the computer disk drives when a system is unattended.

4. Use a password-protected screen saver when a computer is unattended, and password protection for boot devices.

5. Have disk storage guidelines, and follow them when the disks are not in use.

6. Conduct frequent inventories of disks containing sensitive information.

7. Implement a process for backing up sensitive project information and store the backup media appropriately (for example, at a protected off-site location).

8. Use operating system-provided protection measures to isolate sensitive information from non-sensitive information.

9. If possible, use either encrypted passwords (as with Kerberos), or single-use passwords (as with smart cards). If multi-use passwords are used, then select difficult passwords or, better yet, use machine-generated

passwords. Change the passwords frequently. Do not share pin numbers or passwords and protect them from compromise.

6.4 Information Handling

6.4.1 Basic Practices

Project personnel are responsible for ensuring that sensitive information is handled correctly. They should:

- secure sensitive information from unauthorized access;
- inform all involved employees that the information is sensitive;
- control distribution to those with an established need-to-know;
- ensure that sensitive information is identified and marked appropriately;
- date stamp and initial sensitive information received from the customer; and
- properly return or dispose of sensitive information when it is no longer needed.

6.4.2 Project Segregation

When a project personnel is participating in more than one contract or agreement involving sensitive information, the information should be segregated. Information concerning one agreement should always be kept separate from any other sensitive information. This segregation includes but is not limited to discussions, handling, and storage of sensitive information.

6.4.3 Receipt of Sensitive Information

Sensitive information generated by and received from the customer should bear the appropriate markings before it is sent to LANL. It is the responsibility of the customer to identify and mark all sensitive information appropriately. However, if sensitive information is presented unmarked, the individual providing the information is subject to the following guidelines:

- As soon as possible after the presentation, confirm in writing to the LANL Project Leader and project Security Administrator that the information is sensitive, and
- Confirm how the information should be marked and protected.

6.4.4 LANL-Generated Sensitive Information

Information generated and produced by LANL and identified by the customer as sensitive (as noted under the project contract or agreement), should be marked appropriately. Note that markings for other government agencies may have different meanings than those in use at LANL. Be aware of and understand the differences, and handle accordingly.

6.4.5 Document and Media Markings

The top of each page of a document containing sensitive information should be stamped with the appropriate markings, according to the requirements of the project contract or agreement, or to applicable law or regulation. Markings that restrict dissemination of the information should appear on the title or first page of the document before distribution. If the document is generated electronically (as most are), the appropriate markings should be properly placed on the document and all media from the time of its inception. Examples of sensitive information document markings are:

- **Official Use Only** or **OUO**. This marking is used for internal Laboratory personnel rules and practices, proprietary information obtained from companies working with the Laboratory, and personnel and medical files.

- **Export Controlled Information** or **ECI**. This marking is used for information that is export controlled by Federal Regulation.

- **Privacy Information, Private,** or **In Confidence**. These markings usually denote information that is protected from public disclosure or release to unauthorized individuals, such as personnel and medical files.

- **Protected CRADA Information.** This marking is used for private technical, financial, or business information that is provided to, acquired by, or controlled by the Laboratory, or is generated by the Laboratory in connection with a Cooperative Research and development Agreement (CRADA).

All electronic media containing sensitive information (e.g., tape, CD-ROM and diskette) should be labeled **Unclassified Sensitive**.

6.4.6 Information Distribution

The Project Leader should control the copying and distribution of sensitive documentation (such as reports and memos). This responsibility includes recording the number of copies distributed and maintaining a list of recipients. Before receiving the sensitive information, all recipients should sign an acknowledgment form stating that they will not share sensitive information with unauthorized individuals without prior approval from the Project Leader. The Project Leader should keep all such acknowledgments in the project file. The Project Agreement (Section 7.1) should stipulate project rules for information distribution.

This guide recommends that a the Project Leader ensure the documentation of a procedure establishing the mechanisms for distributing sensitive information. Project personnel should adhere to any such procedures and explicitly document any deviations or anomalies.

6.4.7 Information Storage

Project personnel should maintain sensitive information with a reasonable standard of care to prevent unauthorized access of the information.

In areas where access controls exist, sensitive information not in use should be stored as follows:

- During normal working hours, unattended sensitive information should be left in a locked office.
- At all other times, sensitive information should be stored in a locked container, e.g., a file cabinet, desk drawer, or other repository, which should be in a locked office.

In open areas without access controls, sensitive information not in use should be stored in a locked container, e.g., a file cabinet, desk drawer, or other repository. Outside of normal working hours, this locked container should also be in a locked office.

When individuals who are not authorized to view or hear sensitive information are nearby, care should be taken to prevent unauthorized access to the information.

6.4.8 Information Transmittal

6.4.8.1 Hand Carry

Hand carrying sensitive information within the Laboratory site provides more protection than sending such information by insecure electronic means.

6.4.8.2 Snail Mail

A secure way of transmitting sensitive information is through the Laboratory mail system, the US Postal Service, or private delivery services (e.g., Federal Express). If sensitive information is to be sent this way:

- be certain the recipient of the mail is authorized to receive sensitive information;

- wrap the information to prevent disclosure of the contents and the sensitive markings;
- place the information in an opaque envelope, seal the envelope and address it; and
- mark the outer envelope "To Be Opened By Addressee Only."

Certified or Registered mail is an effective way to ensure delivery to a specific, authorized individual.

6.4.8.3 Electronic Mail/FAX

If possible, do not use unencrypted Faxes or email to transmit sensitive information. Keep in mind that all unencrypted FAX or email transmission is extremely insecure. Unencrypted email over unpoliced networks such as the Internet provides a negligible level of information protection. Any message passes through multiple, unprotected hosts and may be routinely backed up at both ends (and may therefore be accessed by system personnel without a need-to-know). Unencrypted Faxes provide a low level of information protection. The transmission mechanisms are not protected and the Fax may accidentally be sent to the wrong destination.

When using FAX or email to transmit sensitive information:

- Only authorized persons (those with a need-to-know) should transmit or receive the information.
- Do not send sensitive information to general email distribution lists.
- Use extreme care in addressing email and dialing FAX numbers, to ensure that sensitive information is not sent to an incorrect location.
- All copies of FAX messages containing sensitive information should be immediately removed from both the outgoing and incoming FAX machines by authorized persons. A telephone call will ensure that an authorized person is standing by on the receiving end so that sensitive information does not sit for some time in the incoming hopper and does not get picked up by an unauthorized individual.
- Explore what happens to email messages, both on the transmitting and receiving ends. Many systems automatically back up all email messages, where they may be readily available to unauthorized individuals.

Where possible, encrypt electronically transmitted sensitive information. In the case of Unclassified Controlled Nuclear Information (UCNI), such electronic transmissions must be encrypted when using public communication lines. However, encrypted information is decoded at the destination, so you should know who has access to that destination, and you should establish the need-to-know for all recipients at that destination.

6.4.8.4 Telephone

When using a non-secure telephone to discuss sensitive information:

- Never discuss sensitive information on cellular or cordless telephones.
- Keep telephone discussions of sensitive information to a minimum.
- Keep in mind that others may overhear the conversation; be aware of the surroundings.
- Never leave messages containing sensitive information on voice mail.
- Be certain the person or persons being talked to are authorized to receive sensitive information.

If possible, encrypt telephone calls involving sensitive information.

6.4.8.5 Video Teleconferencing

When having non-secure video conferences to discuss sensitive information:

- Keep discussions of sensitive information to a minimum.
- Keep in mind that others may overhear the conversation; be aware of the surroundings.
- Be certain the person or persons being talked to are authorized to receive sensitive information.

If possible, encrypt video teleconferences involving sensitive information.

6.4.9 Information Reproduction

Procedures for disseminating sensitive information should be followed when distributing reproduced information. Do not use reproduction service bureaus for making copies of sensitive information. The LANL Copy Center, however, is trained in the reproduction of sensitive unclassified (and classified) information.

Use the following guidelines when duplicating information.

- Reproduced sensitive information should bear the same markings as the original.
- Make only as many copies as the project requires.

- Check for any copies that may be left inside the copy machine or collator.
- Check to be certain that you have the original before leaving the copy machine.
- Treat waste copies (even if only partially legible) as sensitive waste (see Section 6.4.9).

6.4.10 Information Destruction

When customer-provided sensitive information is no longer needed, the Project Leader should ensure that it is returned to the customer or destroyed, as stated in the contract or agreement. Sensitive information in any form should *never* be discarded in regular wastepaper or trash containers.

6.4.10.1 Documents

LANL-generated sensitive documents not retained under the contract or agreement or returned to the customer should be disposed of by:

- Shredding (Classified or Unclassified shredders), or
- Placing into Sensitive Information destruction containers that are handled in accordance with established information destruction procedures.

6.4.10.2 Media

Media such as diskettes or tapes containing sensitive information should be sanitized, degaussed, or destroyed.

6.4.10.2.1 Operable Media

Responsible personnel should:

1. Sanitize the disk by writing over all blocks twice, first with zeros, and again with ones. Use of the "government wipe" option in Norton Utilities, Mac Tools, Unishred or other such tools satisfies this requirement. Contact your OCSR and/or Property Administrator for Assistance.
2. Remove all labels from the disk only after the media is sanitized.
3. If it has a property number, contact your Property Administrator for assistance in completing a sanitization form.

6.4.10.2.2 Non-Operable Media

Responsible personnel should:

1. Ensure that the disk is destroyed. Acceptable methods include:

   A. Degaussing with a Type 1 degausser. The LANL Central Computing Facility (CCF) has an approved degaussing facility (the only one at the Laboratory), and the CCF Operations Desk will accept diskettes for approved destruction. Contact Reuben Roybal, CIC-17 at 7-4584/rrr@lanl.gov.

   B. Destroying by pulverizing, smelting, incinerating, disintegrating, or other mechanism to ensure that the media is physically destroyed. Contact your Property Administrator for further guidance.

2. Deliver for degaussing or destruction with the disk still labeled.

3. If it has a property number, contact your Property Administrator for assistance in completing a sanitization form.

6.5 Connectivity

The safest sensitive information processing is that performed in an environment that is physically and electronically isolated from systems and personnel without the appropriate need-to-know. Computers that are not connected to each other at all, or are isolated to the physical confines of a small laboratory, do not have the security problems of those connected to a large-scale network such as the Internet. An isolated computer or Local Area Network (LAN) can be effectively limited to a small set of users with need-to-know. On the other hand, the Internet connects thousands of machines and millions of users on every continent in the world. This potentially exposes every computer on that network to any one of those millions of users. It is a good rule of thumb to assume that any computer or workstation on a LAN directly connected to the Internet can readily be compromised.

.This section provides a summary of the various connectivity choices available to projects that process sensitive information.

6.5.1 Dedicated, Isolated Computer

An isolated, individual computer (i.e., not connected to any network) is an environment where:

- the computer is dedicated to a single project;
- one or multiple authorized users are allowed at a time;
- all users are authorized to access all information on the system;
- the computer is physically protected; and

- whether single or multi-user, the computer is used only by personnel with need-to-know for the project.

This configuration provides a high level of information protection. However, it does not allow any interconnectivity to other computers or network services.

6.5.2 Dedicated, Isolated LAN

Sensitive processing may be done on an electronically isolated and physically protected local area network (LAN). This environment may be used by personnel who do not have the security clearances required for the Secure ICN (such as those with Graduate Research Assistant and Post-Doctoral positions). This is an environment where the LAN:

- is dedicated to a single project;
- is electronically isolated from any other network;
- has all nodes physically protected; and
- is limited to personnel with explicit need-to-know for the project

This configuration provides high levels of information protection. In addition, it allows the convenience of interconnectivity between project personnel. However, this choice does not allow connections to services outside the local area network.

6.5.3 Computer Connected to the LANL Protected Open Network

The LANL Protected Open network is connected indirectly to the Internet through a perimeter network[3], which is a kind of firewall[4]. This perimeter network isolates inside users from the Internet by using proxy servers[5] to relay requests and answers between them and the Internet. Employing traffic separation, sections of it can be virtually isolated to provide need-to-know separation. Access to it requires the use of smart cards that feature single-use passwords. It provides the convenience of limited connectivity to the Internet world of information, while protecting against the worst of its dangers. While use the Protected Open Network is a calculated risk, the provided protections mitigate this risk to a considerable degree. The Protected Open Network is

[3] A network added between a protected network and an external network, in order to provide an additional layer of security. Sometimes called a DMZ (De-Militarized Zone).

[4] A component or set of components that restricts access between a protected network and an external network.

[5] A program that deals with external servers on behalf of internal clients.

limited to those personnel having a clear need to use it. It thus is a useful area in which to perform unclassified but sensitive work.

6.5.4 Computer Connected to the LANL Wide Open Network

The LANL Wide Open network is directly connected to the Internet, and thus provides the convenience of virtually unlimited connectivity to the Internet world of information, and a maximum of flexibility to its users. However, also because of this connectivity and flexibility, there is no guarantee of information protection. Using systems or subnets of the Wide Open Network for processing sensitive information is a considerable risk, and should not be taken lightly.

6.5.5 Modems

Modems are devices that connect a computer and terminal through an ordinary telephone line. Modems introduce security risks because they allow anyone to call a computer having one. Also, once a modem is in use, a standalone computer or isolated LAN is no longer separated from the rest of the world. Protection against external access may be ensured by physically disconnecting the modem from the telephone and computer when not in use. Be aware of the dial-in and dial-out capabilities of your modems.

6.6 Uncleared Visitors

Laboratory visitors are escorted within secure LANL areas. However, in open areas the following precautions should be taken:

- Visitors should be kept from areas where they can see sensitive information.
- Visitors should be escorted at all times when entering or in an area containing sensitive information.
- Be cautious when answering questions that may involve sensitive information.

6.7 Outside the Work Area

6.7.1 Conversations in Public Places

Use extreme care not to discuss sensitive information outside appropriate LANL work areas. Unauthorized persons may overhear conversations in the LANL hallways, parking lots, cafeterias, lavatories, and public places such as restaurants and commercial airlines.

6.7.2 At Meetings and Conferences

Apply the appropriate security considerations before discussing sensitive information in meetings and at conferences:

- Make sure that all attendees are authorized to receive the sensitive information.
- Advise participants that sensitive information is being discussed and remind them of their responsibility to protect it.
- Do not leave sensitive information unattended or on chalk boards, white boards, easels, flip charts, etc.
- Do not leave sensitive information in unattended meeting rooms. Even locked meeting rooms are not secure because many unauthorized people may have the keys to such rooms.

6.7.3 On Travel

When it is necessary to take sensitive information on travel, take care to maintain control of the information:

- Take only the sensitive information actually needed.
- Keep the sensitive information in your direct possession, in a locked briefcase. Do not check the briefcase or leave it in your hotel room unattended.
- Do not read or expose documents containing sensitive information on an airline or in any other public place.
- When you leave your hotel room, carry the sensitive information with you or have it locked in the hotel safe.

6.8 Disaster Recovery

One of the most important things that can be done to protect information from a disaster is to plan for that disaster. Each project should have a strategy for keeping computer equipment and information available in case of an emergency. Possible emergencies include an office fire, flood (e.g., overhead sprinklers going off), or a major disk crash. Disaster preparedness might include such activities as backing up data for storage at a remote site, and arranging for the use of other computer facilities or equipment to ensure uninterrupted access and availability. Such arrangements may be informal (e.g., a reciprocal agreement with another organization to use each others' equipment) or formal (e.g., preparing a separate emergency site or contract with an organization that handles disaster preparedness). Besides protecting equipment and information, such a plan will greatly increase customer confidence in the LANL ability to safeguard sensitive information.

6.9 Operational Security

Operational Security, also known as OPSEC, is the final component of the protection suite. The term describes measures that delay or deny an adversary hoping to exploit unclassified pathways to critical and sensitive information via aggregation (gathering of large quantities of information) and inference (looking for patterns and building larger conclusions from analysis of the aggregated information). The information protected by OPSEC measures may be classified or unclassified.

It is each employee's responsibility to be aware of the possible avenues for inadvertently revealing sensitive information. Did you ever think of your wastebasket, recycle box or discussions in public places as a good source of sensitive information? The pieces of information revealed by these sources might not be sensitive in and of themselves, but added to other information (aggregated) might reveal the next big hardware purchase or who has the best bid for the next database server contract.

Ask yourself these questions before you route or discard documents:

- *Would an adversary like to have this information?*
- *Could this be the "missing puzzle piece"?*
- *Is all of this information necessary? Can I leave some of it out?*
- *Who really needs to get this information?*
- *How should I handle this information?*

6.9.1 OPSEC Guidance on Disposal of Sensitive Information

Be conservative about producing hardcopies of sensitive information. Where you don't have a piece of paper, disposal is not a problem. The following documents should be shredded or placed in a Burn Box:

1. Documents marked: "SECRET", "Not for Public Release", "Official Use Only", or "In Confidence".

2. Privacy Act information including: dates of birth, place of birth, Social Security number, marital status, sex, home address and telephone numbers, medical information, personnel action memos, and personal credit card and bank account numbers.

3. Payroll, Litigation, and Proprietary information, Cost and Program Codes, sensitive procurement forms, Security reports on division programs, Equipment Security plans, executive summaries on projects.

Documents containing only a Z number and an associated name may be recycled. However, if any other of the above information is also contained in the document it may not be recycled.

7. DOCUMENTATION

7.1 Protection Agreement

While previous Sections detail the protection mechanisms required by LANL, a customer may decide to vary from this recommended standard, and may impose a more, or less, rigorous standard. The information owner has a right to do this. However, whatever it is, the criteria adopted for each project should be fully documented. This documented understanding should be signed by the information owner and by all LANL personnel on the project. What follows is an example of a project agreement:

Project Information Protection Agreement
between XYZ Company and
Los Alamos National Laboratory, Group ZZZ-4
for the Gizmo Project

1. *Project data*. In this project we deal with two kinds of data. The first is private party data from the customer. This kind of data is highly sensitive because of privacy issues. We have already received guidance from our customer on how to protect it. This document concerns the protection of non-private data. This includes project memos, minutes, and other documents.

2. *Sensitive vs. non-sensitive.* Some non-private data should be considered sensitive, and some non-sensitive. Sensitive non-private data describes project techniques and their effectiveness. Examples are the project White Paper, which lays out our technical approach, and memos giving success or failure rates for different techniques. Examples of non-sensitive data are project minutes (assuming they are sufficiently vague), memos regarding trip or meeting planning, and our "who's who" list of project personnel.

3. *Who decides?* The person who produces a non-private document has the responsibility of determining whether it is sensitive or non-sensitive using the project sensitive information criteria. If uncertain, please consult John Doe or Jane Zoe.

4. *Non-sensitive data*. Non-sensitive data can be processed and stored on a machine connected to the Internet. It can be freely e-mailed over the Internet, mailed, or FAXed. It does not require special headers or footers.

5. *Isolated systems*. Sensitive non-private data can be stored on a stand-alone machine or LAN from which the Internet cannot be accessed. The following procedures should be followed:

- if data are stored on a LAN, all users of the LAN should have a common need-to-know
- the machine(s) should be password-protected
- the machine(s) should have password-protected screen savers
- the machine(s) should be physically protected to a reasonable degree; e.g., doors should be locked when the room is vacated.

6. *Sometimes-connected machines.* Sensitive non-private data can be processed, but not stored, on a machine from which the Internet can be accessed (e.g., a Macintosh from which you can access an open LAN through Versaterm). The following procedures should be followed:

   - data should be kept on a diskette, or encrypted on a hard disk, except during active processing
   - diskettes (if used) should be kept in a locked drawer when not in use
   - Internet access should be prevented during processing, either physically (unplug the connection) or logically (e.g., on a Macintosh, quit Versaterm, Netscape, or any other software running Mac TCP; file sharing should be turned off). Please consult someone familiar with your hardware and software to find out the appropriate procedures for your machine.
   - Run virus scanning software against your computer before processing sensitive information.

7. *Always-connected machines.* Sensitive non-private data cannot be stored or processed on a machine that maintains a continuous connection to the Internet.

8. *Email.* Sensitive non-private data cannot be sent across the Internet.

9. *Hardcopies.* Sensitive non-private data should be marked "Official Use Only" in the top and bottom margins. Hardcopies should have a tightly controlled circulation (customer, project personnel, accountable managers). Drafts and extra copies should be shredded after use.

10. *Faxing.* Our customer's practice allows the faxing of sensitive non-private information. Please do this as little as possible. As an alternative, consider hardcopy mail channels or editing out sensitive portions of documents. When the timely nature of a sensitive document requires it to be FAXed, you should notify the receiving party before the fax is sent, and ask him or her to call back if the fax is not received.

11. *LANL mail.* Sensitive non-private information can be sent through Laboratory mail, or left in a mailbox, in a sealed envelope marked TO BE OPENED BY ADDRESSEE ONLY.

12. *Hardcopy mail.* Sensitive non-private information can be mailed through the Postal Service or Federal Express. For extra protection, enclose the document in a second, inner, sealed and addressed envelope marked TO BE OPENED BY ADDRESSEE ONLY.

13. When the project is completed the private party data and documentation from the customer will be returned. With the exception of a protected archive of historical information, all information pertaining to this project will be removed from workstations and computers, and all hardcopy and media will be destroyed.

____
XYZ Company Rep Date

____
LANL Project Leader Date

____
Project Member # 1 Date

⋮

____
Project Member #x Date

7.2 Protection Mechanisms

The agreed-upon protection mechanisms should be documented in procedures that specify the steps that implement those protection mechanisms. All project personnel should be trained in the execution of those procedures.

7.3 Need-to-Know

Every project should document for all project personnel the mechanism(s) by which need-to-know is conferred, and to whom. This document also should specify the minimum criteria that should be met by anyone who is granted the need-to-know.

8. REFERENCES

8.1 DOE Orders

[1] DOE 1240.2A, Unclassified Visits and Assignments by Foreign Nationals, Attachment 5, "Sensitive Subjects"

[2] Unclassified Automated Information System Security Program (Department of Energy Order 1360.2B, Office of Administration and Management, April 1992)

[3] DOE 1360.7, Use of LANL-owned computers off-site. Use LANL-owned or privately owned computers on or off site.

[4] DOE 1430.1D, Scientific Information and Technical Information Management.

[5] DOE 1700.1, Freedom of Information Act (FOIA) Exemptions

[6] DOE 1800.1A, Privacy Act

[7] DOE 5630.3, Identification of Unclassified Controlled Nuclear Information (UCNI)

[8] DOE 5635.1A, Document Markings

[9] DOE 5635.4, Protection of Unclassified Controlled Nuclear Information (UCNI)

8.2 Legislation

[10] California Information Practices Act (CIPA)

[11] Uniform Trade Secrets Act

[12] Privacy Act of 1974 (PA)

[13] Public Law 100-225

[14] The Computer Security Act of 1987

[15] The Atomic Energy Act of 1954

[16] The Arms Export Control Act

[17] The Export Administration Act of 1979

8.3 LANL Documents

[18] LANL Administrative Manual (AM), Section 700, Subject 708, Information Practices

[19] LANL Administrative Manual (AM), Section 700, Subject 721, Conflict of Interest: Privileged Information

[20] LANL Office Procedures Manual (OPM), Section 1, Unclassified Documents, Subject 1, Unclassified Administrative Markings

[21] Computer Security Handbook, FSS Division, April 1994.

[22] Unclassified Sensitive Information Identification and Protection Manual, Los Alamos National Laboratory, FSS Division, Draft, November 1995

8.4 Federal Regulations

[23] 10 CFR Part 110 controls the export and import of nuclear equipment, material, and technical information

[24] 10 CFR Part 810 controls assistance to foreign atomic energy activities

[25] 22 CFR Part 120 provides the International Traffic in Arms Regulations (ITAR)

[26] 15 CFR Parts 730-799 contains the Export Administration Regulations (EAR)

[27] 10 CFR 810 specifies what assistance may be given to foreign atomic energy activities, and under what circumstances

9. GLOSSARY

This Section establishes definitions for the terms and acronyms used in this guide.

accountable manager A LANL manager or designee responsible for an operation, program, project, process, or facility.

burn box A container designated for disposal of sensitive or critical information, the contents of which are protected until either shredded or incinerated.

CIC Computing, Information, and Communications (Division).

CRADA Cooperative Research And Development Agreement; a contract between The Regents of the University of California/LANL and nonfederal parties that *may* result in the exchange of information that:

- embodies trade secrets developed at private expense outside the CRADA agreement,
- contains commercial or financial information that is privileged, or
- is proprietary information.

customer The buyer of a service from LANL.

disaster recovery plan Includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster.

information steward An individual having administrative oversight for the information; having obtained this responsibility from the information owner. The information steward is responsible for:

- Designating a team or individual as the ongoing point of contact within the organization;
- Transferring stewardship to another organization if necessitated by programmatic shifts, organizational restructuring, etc.;
- Operational management of the information, including:

- verifying the information upon receipt, and assuring the continuing integrity of the data, including performing updates and correcting errors;

- providing adequate backup capabilities and appropriate access controls;

- ensuring availability to authorized users;

- maintain appropriate documentation.

information owner The person who currently has legal possession of the information.

information stewardship
The responsibility for managing information. For the assigned information, the steward ensures accuracy, performs updates and corrections as needed. protects the information from accidental loss or security violations, and is the primary point of contact for anyone attempting to access the information.

information user Anyone directly interacting with the information.

Laboratory Los Alamos National Laboratory

LANL Los Alamos National Laboratory

Los Alamos Los Alamos National Laboratory

need-to-know A protection principle stating that a user should have access only to the information he or she needs to perform a particular function.

OCSR Organizational Computer Security Representative.

security administrator An individual on each project that handles sensitive information who is responsible for security administration on that project. This individual will have the responsibility and should have the authority to ensure that project personnel adhere to the requirements covered in this guide.

sensitive information Certain unclassified information requires some degree of protection from disclosure to unauthorized persons, from unauthorized alteration, and from loss.

WFO agreements Work-For-Others agreements. WFO is undertaken when the proposed work requires the use of capabilities and/or facilities unique to LANL and does not interfere with LANL priority use of the same personnel and facilities. WFO agreements cover any work that:

- Is performed for nonfederal parties,
- Uses LANL facilities and/or personnel, and
- Is not directly funded in whole or in part by the DOE.

10. WHERE TO GET ASSISTANCE

This Section lists contacts for information sensitivity questions you may have.

- **Your Organizational Computer Security Representative (OCSR).** This individual is available to answer questions regarding computer security and information sensitivity. Your *System Users Computer Security Responsibilities* agreement lists your OCSR by name along with a phone number.

- **CIC-17, Computer Operations Center, 505-667-4584.** The Operations Center will degauss and destroy magnetic media containing sensitive information when it is no longer needed.

- **CIC Division Security Officer, 505-667-9904.** This individual implements the security program for the Computing, Information, and Communications Division, and directs the efforts of the local CIC OCSRs.

- **FSS-DO, Safeguards and Security Program Planning and Management, 505-667- 5911.**

- **FSS-14, Unclassified Computer Security Requirements, 505-665-1795.** This group administers the Laboratory's Computer Security Program and can answer questions regarding the Unclassified Computer Protection Policy, definitions of computer security terms, and provide interpretations of Department of Energy requirements regarding computer protection.

- **FSS-15, Unclassified Sensitive Information Markings, Protection, and Control, 505-665-1803.**

- **FSS-16, Unclassified Sensitive Information Identification/ Guidelines, 505-667-5011.**

- **AA-OPSEC, The Operations Security (OPSEC) Program, 505-665-3372.**

Report Number (14) LA-UR--97-5197

Publ. Date (11) 199611

Sponsor Code (18) DOE/MA, XF

UC Category (19) UC-900, DOE/ER