Unclassified Sensitive Information Protection

Guidelines for Project Leaders

Steve Donahue, 505-665-8630, scd@lanl.gov

Los Alamos National Laboratory, Los Alamos, NM 87545

Release identifier: LAUR-98-1738

What is Sensitive Information?

Information that, if disclosed to unauthorized individuals, or is destroyed or lost, would:

- negatively affect the information owner;
- jeopardize project operations; or
- require substantial resources to recreate.

There may even be criminal or civil penalties associated with sensitive information loss or disclosure to unauthorized individuals.

Responsibilities

Sensitive information must be protected against loss or unauthorized disclosure.

Ultimately, however, the information is created to be of use.

Your obligation is to apply *due diligence* to providing *appropriate* and *reasonable* protection.

Sensitive Information Issues

- Types of information a project has
- Information owners, stewards, users
- Regulatory or customer requirements
- Access requirements
- Protection measures
- Costs / benefits / risks

Sensitive Information Types

- Federal and State Laws
  - Privacy Act, CIPA
  - FOIA, CPRA
- DOE Regulations
  - UCNI, OUO, C/FGI-MOD, Mission Essential
  - ECI, AT, S&T, DUSA
  - Proprietary/CRADA
- Site/Local Policy
  - Administrative, Pre-Publication Drafts

Levels of Sensitivity

- High: Significantly affects DOE or Nation

  Examples: Life-Critical, Mission-Critical

- Medium: Significantly affects Laboratory

  Examples: Mission-Essential, Official Use Only, Privacy Act, UCNI

- Low: Significantly affects owner

  Examples: Proprietary, CRADAs, Administrative, Pre-Publication

- Very Low: No requirement; little adverse effect

  Examples:DUSA, Uncontrolled (Cafeteria Menu)

Risk Assessment

Examine the following:

- Your project's needs
- Costs of losses: to you, your site, customers
- Current information vulnerabilities
- Legal and regulatory requirements

A customer's decision not to protect information as required by law does not absolve you from legal liability.

Access Requirements

- Hardcopy vs. on-line
- Physical locations
- Timeliness
- Need to know
- Distribution between sites
- Reproduction

Establishing Protection

- Establish who is Responsible for Security
- Identify the Sensitive Information
- Rank the Sensitive Information
- Assess the Associated Risks
- Evaluate Protection Mechanisms
- Document Your Decisions and Agreements
- Periodically Revisit Your Decisions

Protection Measures

- Personnel Screening
- Need to Know
- Project Segregation
- Labeling & Storage
- Reproduction & Destruction
- Distribution
- Connectivity
- Continuity of Operations

Protection Regimes

- Protection Regime 3: Robust Authentication, Authorization, and Encryption
- Protection Regime 2: Robust Authentication and Authorization
- Protection Regime 1: Simple Authentication
- Protection Regime 0: Unrestricted Dissemination

Protection Documents

- Protection agreements
- Protection plans
- Implementations
- Authorizations
- Where to get help

Revisiting Your Protection

Maintain proper awareness of your sensitive information, protection needs, and implementations, because *Circumstances Always Change:*

- Information sensitivity
- Protection technology
- Project funding
- Understanding of the issues

Unclassified Sensitive Information Protection

Guidelines for Project Leaders

Steve Donahue
Los Alamos National Laboratory
505-665-8630, scd@lanl.gov