



Information Security

Susan Caskey

International Security Programs

February 5, 2004



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.





Agenda

- **What is information management?**
- **What are information assets?**
- **Risk assessment process for information**
- **Mitigation of information security risks**
- **Summary and discussion**



Information Management

- **What is information?**
 - Information is any knowledge which can be communicated or documented regardless of its physical form

- **What is information management?**
 - Manner in which information is governed to achieve efficient and controlled use
 - Includes information security

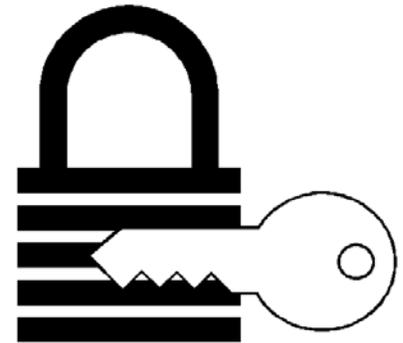
- **What is information security?**
 - A mechanism used to protect the integrity of and access to specific kinds of information





Categorizing Information Assets

- **Categorizing sensitivity levels of information should be based on its potential to damage organization, state, federal, or international biosecurity mechanisms if disclosed to unauthorized persons**
- **Sensitivity levels**
 - Low (open or public information)
 - Moderate (limited access information)
 - High (exclusive or strict access information)
- **Some examples of information assets:**
 - Personnel information
 - Facility details
 - Physical security information
 - Network security information
 - **Specific information on High Consequence Pathogens and Toxins (HCPTs)**
 - Databases
 - Lab records
 - Security procedures
 - Scientific papers





Risk Assessment Process for Information

- 1. Define the information assets**
 - Context and sensitivity
- 2. Evaluate consequences of loss**
 - Physical access to facility
 - Detailed understanding of transfer process which can aid in theft during transfer
 - Listing of person's with access to HCPTs
 - Details of target locations
- 3. Categorize the sensitivity of information assets**
 - Low
 - Moderate
 - High
- 4. Identify the adversaries**
 - External
 - Internal
- 5. Assess the manner in which the adversaries could acquire the information**
 - Physical break in
 - Offsite storage
 - Trash
 - Network attack
 - Accidental release
 - Intentional release
- 6. Evaluate the risk**
 - Prioritize the scenarios



Mitigation of Information Security Risks

● Policies



- Policies should be realistic and complete
- Specific policies and procedures should be created for any electronic data

● Practice



- By the creation of realistic policies, people will be more likely suited to follow the policies

● Training



- People need to be kept knowledgeable about information security
- People need to be kept abreast to the changing world of threats and solutions when these factors influence organizational policies



Mitigation of Information Security Risks

Policy Principles



- **No person should have access to moderately or highly sensitive information unless that person has been determined to have a valid need-to-know**
- **The determination of whether an individual has a valid need for information rests with the individual who has authorized possession, knowledge, or control of the information and not the recipient**
- **Information should be identified and labeled based on the level of sensitivity**
- **The physical control of information should be consistent with the level of sensitivity of the information**
- **Transmission and reproduction of this information should follow a consistent practice with the level of sensitivity**
- **A good Information Technology (IT) program is critical to the protection of information, especially when information is available electronically**



Mitigation of Information Security Risks

Policy Details: Identification



- Users of information should know the information's designated sensitivity level
- Levels of sensitivities should be based on standards
 - Low
 - Moderate
 - High
- A review and approval process aids in the identification of sensitivities
 - Critical for public release of information





Mitigation of Information Security Risks

Policy Details: Marking



- Moderately and highly sensitive information should be labeled in a consistent manner
 - Sensitivity level designation
 - Top and bottom of each page / cover sheet
- Marking and control methods should be well understood by those working with information

Moderate

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

December 1, 1995

MEMORANDUM FOR: David Smith, Chief
Division 5

From: Susan Goode, Director

Subject: (U) Recommendations for
Resolving Funding Problems

1. (S) This is paragraph 1 and contains "Secret" information taken from paragraph 2 of the source document. Therefore, this portion will be marked with the designation "S" in parentheses.

2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

3. (U) This is paragraph 3 and also contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

Derived from: Memorandum dated 11/1/95
Subj: Funding Problems
Department of Good Works
Office of Administration

Declassify on: December 31, 2000

Moderate

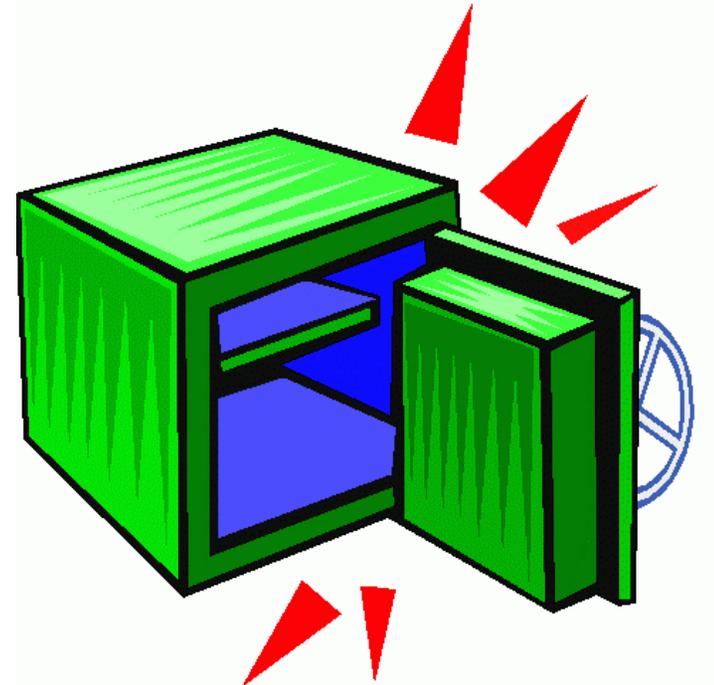


Mitigation of Information Security Risks

Policy Details: Control



- The control of moderately and highly sensitive information should be the direct responsibility of the individual with the information
- This includes the physical security of the information and places where the information is stored



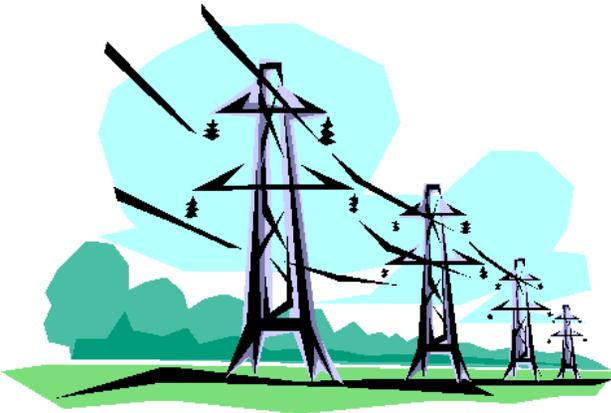


Mitigation of Information Security Risks

Policy Details: Transmission



- Insecure transmission of information can lead to accidental release
- Transmission should only occur via approved methods
 - Mail, email, or fax security is required
 - Limited discussions in open areas
 - Information should only be reproduced when needed and each copy must be controlled as the original





Mitigation of Information Security Risks

Network and Desktop Security Policy Details



- **Network policies**
 - The network on which all information is transmitted should be protected

- **Desktop policies**
 - Each system within the network should maintain a level of security

- **Transmission policies**
 - The transmission of moderately or highly sensitive information can be done securely on the internet, but must follow basic transmission policies





Mitigation of Information Security Risks Practice



- **Realistic policies**
 - Policies should be comprehensive
 - Policies should allow for users to work as needed

- **Understanding of policies by all users**
 - Having clear policies is critical to users following them
 - The policies should be easy to locate, understand, and follow



Mitigation of Information Security Risks Training



- **Training on policies**
 - All users should have training on policies, especially those policies that affect them directly
 - Training needs to be provided in a manner that does not disrupt work, yet reminds users of the criticality of information protection

- **Specialized training for some**
 - People directly working with HCPTs may require additional training
 - The IT staff should be trained to know what the realistic network threats are



Summary

- **Information security is critical to biosecurity**
- **Information at risk may include:**
 - Personnel information
 - Facility details
 - Specific information on High Consequence Pathogens and Toxins (HCPTs)
 - Security procedures
 - Scientific papers
- **Information security is comprised of understanding:**
 - Levels of sensitivity
 - Risks to information
 - Information policies
 - Practice and training