SAND--88-3114

DE89 008995

Distribution
Category UC-15

IMPLEMENTING SECURITY MEASURES FOR COMPUTER-BASED SECURITY SYSTEMS

Debra A. Faculjak
Facility Systems Engineering Division 5245
Sandia National Laboratories
Albuquerque, New Mexico 87185

ABSTRACT

Directorate 5200 of Sandia National Laboratories, Albuquerque (SNLA) has provided computer-based security systems to several Department of Energy (DOE) nuclear sites, and to other federal agencies. Because these systems are critical to national security, their computing resources and data must be protected. The purpose of this document is to ensure that system designers (a) become familiar with security issues, policy, and directives, and (b) are able to integrate protection of the computer, its peripherals, and its data into the system.

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.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

ACKNOWLEDGMENTS

I would like to thank Computer Security Division 2612, Sandia National Laboratories, Albuquerque, and the DOE Center for Computer Security, Los Alamos National Laboratory for their helpful contributions and review of this document.

CONTENTS

IMPLEMENTING SECURITY MEASURES FOR COMPUTER-BASED SECURITY SYSTEMS

1. INTRODUCTION

Directorate 5200, Nuclear Security Systems, of Sandia National Laboratories, Albuquerque (SNLA) has provided computer-based security systems to many Department of Energy (DOE) sites and to other federal agencies. These automated data processing (ADP) security systems are critical to ensuring national security. Most of the systems and their data are currently categorized as unclassified. Although system security has always been an important consideration, security was approached on an informal basis because these unclassified systems were being installed in a secure environment at DOE sites.

Since the "Computer Security Act of 1987" became federal law in January 1988, computer security has become an even more important national concern. In light of the new law, a more formal approach should be considered for computer-based security systems. This approach should include adherence to an ADP Security Program, similar to that outlined in DOE Order 5637.1, "Classified Computer Security Program."

1.1 Purpose

The purpose of this document is to ensure that system designers (a) become familiar with security issues, policy, and directives, and (b) are able to integrate protection of the computer, its peripherals, and its data into the system at an early stage in its design. This document provides a comprehensive and uniform review of those security issues that are pertinent to the applications developed within Directorate 5200. The intention of this document is to provide guidance in the development of appropriate computer security protection for the SNLA-developed security systems. The policies and standards of computer security, set forth by the Department of Defense (DOD) and the DOE, are provided to enhance the designers' understanding of the rationale for such security.

1.2 Approach

Although the ADP security systems developed by Directorate 5200 are currently unclassified, these systems and future systems may become classified. The guidelines presented in Chapter 3, the Abbreviated Guide for an ADP Security Plan, are aimed toward a classified system because of the current systems' potential for an upgrade, and because the measures outlined for a classified system are more comprehensive than for an unclassified system. Chapter 4 contains specific actions that should be considered in an unclassified system and are based on the issues discussed in Chapter 3. The guidelines are meant to help the system designer of an unclassified system apply security measures that are also consistent with a classified system.

Please remember that this document is intended to be used only as a guide. References to DOE Orders and other security publications will be included, as necessary, so that you can obtain detailed information on each security topic.

2. WHAT IS COMPUTER SECURITY?

Ideally, the aim of DOE computer security is for its classified ADP systems to be totally secure, i.e., for a system to "protect itself and the information it contains against all threats, known and unknown." In practice, however, the aim of computer security is to protect the computers and the information in them to the best of our ability.*

Computer security is defined as management measures and technological safeguards that are established and applied to protect assets from loss or harmful actions. DOE has developed a program that contains uniform requirements to ensure the security of ADP systems. Under the program, an ADP Security Plan must be developed for each separate system. An ADP Security Plan is a description of the measures used by the site users, the system manager, and the system designer to protect sensitive data and systems, classified and unclassified.

When the DOE refers to an ADP system, the term means (a) the computer hardware, (b) the firmware, (c) the telecommunications, (d) the interconnections with other ADP equipment (e.g., networks), and (e) the entire collection of software that is executed on the hardware. Although the term "system" is occasionally used by the DOE to refer to a set of programs that implement a specific function, computer security must always be applied to the complete ADP system.

According to DOE Order 5637.1, the DOE policy on computer security is as follows:

> *... that classified information and classified ADP systems shall be protected from unauthorized access (including the enforcement of need-to-know protections), alteration, disclosure, destruction, penetration, denial of service, subversion of security measures, or improper use as a result of espionage, criminal, fraudulent, negligent, abusive, or other improper actions.*
>
> *The DOE shall use all reasonable measures to protect ADP systems that process, store, transfer, or provide access to classified information or PARD (Protect As Restricted Data) to include but not limited to the following: physical security; personnel security; telecommunications security; administrative security; and hardware and software measures ...*
>
> *The order establishes the baseline security requirements for the protection of classified ADP systems.*

* Alice L. Baker, "Standards for the DOE Classified Computer Security Program," in A Summary of Papers to be Presented at the 11th Department of Energy Computer Security Group Conference, Kansas City, MO, May 3-5, 1988.

2.1 Baseline Security Requirements

An ADP system requires security in five main areas. Although not all areas are under the control of the ADP security system designer, he or she should have a good understanding of what is meant by and involved in each area. Below are general definitions for these baseline security requirements:

- **Physical Security** -- Physical security involves the use of locks, guards, badges, alarms, procedures, and similar measures (alone or in combination) to control access to the classified ADP system and related equipment. Physical security also refers to the protection of the structures that house the classified ADP system, related equipment, and the contents from espionage, theft, waste, fraud, abuse, or damage by accident, fire, and environmental hazards.

- **Personnel Security** -- Personnel security refers to established procedures for ensuring that all personnel, with access to classified information, have the required authorizations and appropriate clearances. Authorization is also required for unclassified sensitive or private information.

- **Telecommunications Security** -- Telecommunications security comprises two areas: emissions and transmissions.

  Emissions security is the measures taken to deny unauthorized persons information of value if emanations from crypto-equipment and telecommunications systems were intercepted and analyzed. These measures are generally known as TEMPEST requirements.

  Transmissions security requires that approved cryptographic devices or the Protected Distribution System [PDS] be used to protect classified information on communications lines that pass outside the security area of an ADP system or facility.

- **Administrative Security** -- Administrative security is the procedures established to ensure that classified ADP systems and facilities have adequate controls for access to and handling of classified information.

- **Hardware and Software Security** -- Hardware and software security refers to the implementation of a combination of features -- in addition to physical and personnel security -- to provide protection of classified data that are processed, stored, transferred, or accessed via the ADP system. Protection requirements are based on the level of data and user clearance.

These elements are discussed in more detail in Chapter 3 of this document, "An Abbreviated Guide for an ADP Security Plan."

2.2 Protection Index

The DOE declares what the protection requirements are for a classified ADP system by determining its Protection Index. A Protection Index is a measure of perceived risk determined from the combination of the users' clearance levels and the classification of the data on the ADP system. Although the Protection Index is intended for a classified system, it can also be useful in helping to determine security measures for an unclassified system. Currently, the Protection Indexes range from 0 through 3, with an index of 3 requiring the most protection.

The definitions below are taken from DOE Order 5637.1. The term "level of data" means the highest classification and most restrictive category of data on the ADP system. The term "user clearance" means the highest clearance level of the least cleared user.

- *Protection Index 0:* If the "user clearance" meets or exceeds the "level of data" on the ADP system, and all users have a need-to-know all data on the ADP system, the security program must provide identification and authentication, plus the physical, personnel, telecommunication, and administrative controls appropriate to the level of data.

- *Protection Index 1:* If the "user clearance" meets or exceeds the "level of data", but not all users have a need-to-know all data on the ADP system, the security program must provide for access control, audit trail, plus all the requirements of Protection Index 0.

- *Protection Index 2:* If the "user clearance" meets the classification level one level below the "level of data", the security program must provide for internal labels, plus all the requirements of Protection Index 1.

- *Protection Index 3:* If the "user clearance" meets the classification level two levels below the "level of data," the security program must provide for assurance testing, plus all the requirements of Protection Index 2.

The information in Table 1 is taken from DOE Order 5637.1 and shows the current Protection Indexes, with examples of corresponding processing situations.

TABLE 1

DETERMINATION OF REQUIRED PROTECTIONS AND ASSURANCES*

PROTECTION INDEX	EXAMPLE PROCESSING SITUATION	SYSTEM PROTECTION FEATURES AND ASSURANCES	MIN EPL LEVEL**
0	Single user/standalone single level · Single user personal computers (PCs) · Multi-user, common need-to-know (Dedicated system)	Identification and authentication plus physical, telecommunications, personnel, and administrative controls appropriate to the level of the data.	C1
1	Multi-user, not all same need-to-know	Index 0, plus access control and audit trail	C2
2	Partitioned networks, (each partition as a single level) with multi-level processing	Index 0 and 1, plus internal labeling and appropriate ADP system assurance testing.	B1
3	Multi-partition networks, multi-site networks	Index 0, 1, and 2, plus appropriate ADP system assurance testing.	B2
X	NOT ALLOWED	Impractical at this time	

* ADP systems with multiple users, where all users do not have the same "need-to-know", require a minimum protection index of 1.

** If the ADP system to be used is chosen from those listed on the Evaluated Products List (EPL), as published by the National Computer Security Center and specified in DoD 5200.28DTS, the features and assurances provided by the EPL will be accepted as proof of ADP system security capabilities. For other ADP systems, adequate proof of protection of the features and assurances is required. A copy of the most current version of the EPL may be obtained by writing to:

NCSC
National Security Agency
9800 Savage Road
Ft. Meade, MD 20755-6000

2.3 Scope of this Document

When a security system that was developed in-house by Directorate 5200 is placed at another site, a cooperative security effort is encouraged. Although it is the site's official responsibility to ensure that its computer system meets all security requirements, the ADP security systems developed by Directorate 5200 should include built-in security features.* For example, built-in features to accommodate security regulations for telecommunications and hardware/software can be achieved in-house. Whenever possible, the 5200 system designer should develop an understanding of the site's environment so that adequate security features can be designed into the system.

In general, the site is responsible for the physical, personnel, and administrative elements, and the ADP security system designer is involved with the telecommunications and hardware/software elements. However, because responsibilities toward security may overlap in some instances (e.g., administrative controls), a cooperative effort in all areas should be expected. The specific requirements that concern an ADP security system designer are outlined in the next chapter.

* Please note that the DOE Operations Office for each site has the authority to broaden the scope of the existing DOE Orders on computer security. In addition, each site may also require features beyond the specifications of the cognizant Operations Officer.

3. AN ABBREVIATED GUIDE FOR AN ADP SECURITY PLAN

The ADP Security Plan is an integral part of DOE's security program and contains a description of the specific security measures used to protect sensitive data and systems. In general, the development of the plan is the site's responsibility. However, because the ADP security system is itself the focus of the plan, it is important for an ADP security system designer to be aware of its requirements.

This chapter includes information on those sections of an ADP Security Plan that directly relate to the job of an ADP security system designer. This guide to an abbreviated ADP Security Plan is not intended as a fill-in-the-blank format, but rather as a structured approach to how a security plan is developed for a classified ADP system. The system designer is not required to supply all of the information for the sections of the plan presented here, but he or she should be very familiar with their content.

To clarify what should be included in an ADP Security Plan, excerpts from the *Guide for ADP Security Plans: Shared (Multiuser) System*, Los Alamos National Laboratory (Los Alamos, NM: To be published) are presented in Section 3.2, with permission of the authors. However, please notice that only that information from the Guide that pertains to the interests of a designer of ADP security systems is provided. For a complete understanding of the contents of an ADP Security Plan, consult DOE Order 5637.1, the *Guide for ADP Security Plans*, referenced above, and other security-related documents, which are listed in Appendix B.

3.1 Abbreviated Guide for an ADP Security Plan: Contents

Those aspects of an ADP Security Plan that pertain to the ADP security system designer include the following items:

- Narrative Description of the Classified ADP System
  - Description of the System and its Operational Characteristics
  - The Programmatic Mission and Purpose of System
  - Rules Describing Access Controls
- Statement of Threat to the System
- ADP Computer Security Environment Description, including:
  - Protection Requirements Determination
  - Methods to Meet Protection Requirements
  - Level and Amount of Classified Information
  - Architecture of the ADP System
  - Inventory of Hardware and Software Components

- Risk Assessment
- Basis for Certification, including:
  - Physical Security
    - Protection Requirements for Single-Level ADP System
    - Electronic Protection Requirements
  - Telecommunications Security
    - Transmissions Security
    - Emissions Security
  - Hardware and Software Security
    - Protection Requirements
    - Determination of Protection Requirements
    - Features and Assurances

      Access Controls
      Assurance Testing
      Applications Software
      Data Base Management Access Controls
  - Administrative Security for Multiuser ADP System
    - User IDs
    - Authentication
    - Authorization
    - Accountability

Please note that it is not Directorate 5200's responsibility or intent to write an ADP Security Plan, but rather to design security into the systems that are being built.

3.2 Abbreviated Guide for an ADP Security Plan: Issues and Hints

Included in this section are issues and hints that pertain to the ADP plan's contents listed in Section 3.1. This section is intended to provide a system designer with information that he or she must consider early in the development process. The issues and hints are excerpted from the *Guide for ADP Security Plans*, fully referenced above, and identify major points, potential problem areas and vulnerabilities, site-specific considerations, and requirements.

Use the issues and hints as a checklist to review an ADP security system to ensure that its security features are as complete as possible.

3.2.1 NARRATIVE DESCRIPTION OF THE SYSTEM

(provided by the site Computer System Security Officer [CSSO])

This requirement includes a narrative description of the classified system and rules for information access.

- **Description of the System and its Operational Characteristics.**

  A relatively brief description of the system, and the rules for accessing information on it, give the reviewer an overview of the system.

  ISSUES AND HINTS:

  - Give an overview of the system and its relationship to other computing and communication resources at the facility.
  - Make the overview complete.
  - Avoid details, but do not be too brief.

  REFERENCE: *DOE 5637.1, Attachment III-1, 2.c*

- **The Programmatic Mission and Purpose of System** (suggested)

  A comprehensive overview of the mission and purpose of the system provides any reader or reviewer of the security plan with a clear perspective of the overall goals and security environment the system must support.

  ISSUES AND HINTS:

  - Consider giving a complete, comprehensive overview of why the system exists (i.e., its purpose and mission).
  - Consider avoiding technical details without being too brief.

- **Rules Describing Access Controls**

  These rules must describe how information access will be controlled based on the classification level of the information being processed and the clearance and need-to-know of the users accessing the system.

ISSUES AND HINTS:

- Identify the classification level and category of information on the system.
- Explain how the information was identified and how information will be identified in the future.
- Explain how user clearances and need-to-know are determined and how they will be determined in the future.
- Identify user clearances and need-to-know for this system.
- Describe the rules for accessing this system including how future changes to rules will be identified and made.

REFERENCE: *DOE 5637.1, Ch II, 2.a(1),2.a(2), Attachment III-2.c*

3.2.2 LOCAL STATEMENT OF THREAT (provided by the site CSSO)

The local statement of threat for the ADP system must be based on the Site Statement of Threat and must describe all threats unique to the system, which are not addressed in the Site Statement of Threat. If there are no unique threats to this system, then a statement to this effect must be included in the security plan.

ISSUES AND HINTS:

- Reference the Site Statement of Threat for Classified Computers in this security plan.
- Do a complete, comprehensive identification and documentation of all threats to this system.
- Base the local statement of threat on the Site Statement of Threat.
- Identify all threats to the system that are not addressed in the Site Statement of Threat.
- If there are no unique, local threats (i.e., all threats are covered by the Site Statement of Threat), include a statement to this effect.

REFERENCE: *DOE 5637.1, Ch.II, 2.a, Attachment III-1, 2.d*

3.2.3 A DESCRIPTION OF THE ADP COMPUTER SECURITY ENVIRONMENT

The environment description must include, as a minimum, (a) a determination of protection requirements, (b) a description of security-related software and the methods used to meet the protection requirements, (c) the level and amount of classified information, (d) the architecture of the ADP system, and (e) an inventory of the ADP system components.

- **Determination of Protection Requirements** (provided by the site CSSO)
  Describe the process and information used to determine the protection requirements for the system. The description should include an explanation of what protection index was chosen for the system and a complete justification of the chosen protection index.

  ISSUES AND HINTS:

  - Give a step-by-step description of how the Protection Index of the system was determined.
  - You may want to include some of the information collected for the access control rules (see Section 3.2.1, "Narrative Description, Rules for Access Controls").

  REFERENCE: *DOE 5637.1, Attachment III-1,2.e(1)*

- **Description of Security-Related Software and the Methods Used to Meet Protection Requirements.**

  A combination of hardware and software security features, in addition to other measures such as physical and personnel security, are necessary to provide the required protections.

  ISSUES AND HINTS:

  - Give a complete, comprehensive overview of the methods used to meet the protection requirements.
  - If security-related software is used, describe its features and how they help meet the protection requirements.
  - Avoid being too brief, but do not duplicate details from other sections of the security plan.

  REFERENCE: *DOE 5637.1, Attachment III-1, 2.e(2)*

- **Level and Amount of Classified Information** (provided by the site CSSO)

  Describe all levels and categories of information to be processed on the system. The description should be limited to general terms (e.g., Secret Restricted Data -- 30%) and should consider the expected processing activity and the volume of data to be generated, stored, or processed on the system.

  ISSUES AND HINTS:

  - Identify (list) all expected classification levels and categories of information to reside on the system.
  - Precise estimates of amounts of information are not necessary.

  REFERENCE: *DOE 5637.1, Attachment III-1, 2.e(3)*

- **Architecture of the ADP System**

  A graphic depiction (e.g., schematic drawing) of the system showing the organization, interconnection, and interfaces of all system components is necessary to aid the reviewer in evaluating the security plan. The architecture of the system must also include all connections to communications resources and other computing resources.

  ISSUES AND HINTS:

  - Provide a diagram of the system (for the accreditor/reviewer) that shows all interconnections between components in the system.
  - Show all interconnections with other computing resources and communications resources (on-site and off-site).
  - Don't overlook connections that are temporary or used infrequently, e.g., remote diagnostic services.
  - Consider showing the red/black separations as part of the system schematics or on a separate drawing.

  REFERENCE: *DOE 5637.1, Attachment III-1, 2.e(4)*

- **Inventory of the ADP System Components**

  All system components, hardware, operating-system software, and security-related software must be identified. All applications software used on the system should be identified.

  Component-level descriptions for hardware should include each identifiable hardware unit, even if the device is installed in another unit, e.g., memory boards. Software-component descriptions should include each element identified by the vendor or developer, especially any unit containing security functions.

  ISSUES AND HINTS:

  - Include all hardware components, all security-related software, and all operating-system software.
  - Include all applications software with any security-related features.
  - For hardware components, include: location of the component, the manufacturer, model, serial number, property number, any special security features, and any special Tempest characteristics.
  - For software components, include: the developer, proper name of the element, version number, and any security-related features.
  - Consider making the hardware and software inventory an appendix to allow easier updating without affecting the remainder of the plan.

3.2.4 RISK ASSESSMENT (provided by the site CSSO)

A risk assessment, quantitative or qualitative, must be performed on the ADP system in order to create awareness of vulnerabilities and threats.

ISSUES AND HINTS:

- The site must have a risk management program.
- The site risk management program must be based on and correlated with the DOE and local statements of threat.

- The risk management program:
  * identifies hazards, risks, threats, and assets to be protected,
  * performs a risk assessment,
  * reports results for use in the management planning process,
  * documents management's response to the identified risks.
- Risk assessments help ensure that cost-effective, appropriate safeguards are incorporated into a classified system.
- Describe the procedures in moderate detail or reference a document that contains the detail.

REFERENCE: *DOE 5637.1, Chapter II, 2.b*

3.2.5 BASIS FOR CERTIFICATION

This section must give evidence that all the requirements of DOE 5637.1 have been met. The requirements of at least the following areas must be met:

A. Physical Security
B. Telecommunications Security
C. Hardware and Software Security
D. Administrative Security

(NOTE: Personnel Security is a basic security requirement, but is not discussed here because it is considered the sole responsibility of the site.)

A system security test, which maps to the security features of the security plan, can demonstrate that requirements have been met.

ISSUES AND HINTS:

- Cover physical security, telecommunications security, hardware and software security, and administrative security in the security test of the system.
- Plan to test each security feature of the plan and document results, giving details.
- Tests must include verifying that invalid commands are rejected.

REFERENCE: *DOE 5637.1, Attachment III-1, 2.f*

A. PHYSICAL SECURITY

Each ADP system and all peripherals, communications paths, and associated removable media need to be protected commensurate with the highest level and most restrictive category of classified information for which the system is accredited.

ISSUES AND HINTS:

- Consider, in general terms, the procedures for access within the facility and the physical protection measures in use.
- Types of locks and alarms must be DOE approved.
- Determine location of backup systems (e.g., uninterrupted power supply systems)

REFERENCE: *DOE 5637.1, Chapter III, Section 2, DOE 5632.4*

- **Protection requirements for Single-Level ADP systems** (i.e., systems with a Protection Index equal to 0 or 1, or within a DOE Exclusion area). Table 1 in Chapter 2 lists the protection indexes.

  ISSUES AND HINTS:

  - Mention whether the ADP system resides in a vault or a vault-type room.
  - Mention whether there is authorization for open storage of classified information.
  - If the system or components are left unattended or unsecured, describe the disconnection and locking of communications interfaces.

  REFERENCE: *DOE 5637.1, Chapter III, 2.a*

- **Electronic Protection Requirements**

  Each ADP system must be completely separate, physically and logically, from all other systems unless all connected systems are included in a single ADP Security Plan.

ISSUES AND HINTS:

- Each ADP system must be separated from other ADP systems.
- Electronically separate
- Logically separate
- Physically separate

REFERENCE: *DOE 5637.1, Chapter III, 2.e*

B. TELECOMMUNICATIONS SECURITY

Protection of communications resources, e.g., communications links, PDS, is required. The required protection varies according to the Protection Index of the ADP systems connected to the communication resources.

ISSUES AND HINTS:

- Consider whether all components of the system that process unencrypted information reside in a DOE-approved security area.
- Each communication link that leaves the computing resource must be protected according to the highest level of traffic it carries. If all communications links are not protected at the highest level of trafffic carried by any of them, other security measures must be installed to protect data and the computing resources.
- There must be a connect/disconnect procedure to ensure that no data (including residual data) remaining from a previous process are transmitted to an unauthorized individual.
- Unencrypted communications lines must not be connected to any computing resource that processes or stores classified information. (Unencrypted communications lines are allowed in a PDS.)
- Dial-up communications lines must not be connected to any computing resource that processes or stores classified information.
- Physical communications links (e.g., coax, twisted pair, fiber optics, infrared) to and within a computer resource must be documented and controlled under a single management scheme.
- Each communication link supporting a system with a Protection Index of one or zero must be protected commensurate with the level of classification and category for which the system is accredited.

- Each communication link supporting a system with a Protection Index of two or three must be protected according to the highest level and most restrictive category of information carried by that link.
- Maintain red/black separation.

REFERENCE: *DOE 5637.1, Chapter III, Section 2.c, 3; DOE 5300.3A*

- **Transmissions Security**

  ISSUES AND HINTS:

  - Either an NSA-approved cryptographic device or a PDS must be used to protect classified information communicated outside the computing resource facility.
  - A PDS must be constructed in accordance with the DOE PDS guide.
  - The PDS must be managed under a single configuration management scheme.
  - The communications media must be in a DOE security area or a PDS.
  - The security area and the PDS, if used, must be described in the security plan.

  REFERENCE: *DOE 5637.1, Chapter III, 3.a; DOE 5300.4A*

- **Emissions Security**

  ISSUES AND HINTS:

  - Emanations from crypto-equipment, telecommunications, and the ADP system must be reviewed and controlled.
  - A review of or establishment of a TEMPEST Control Zone(s) adequate for the system emanation pattern must take place.
  - Are all cables shielded and properly grounded?

  REFERENCE: *DOE 5637.1, Chapter III, 3.b*

C. HARDWARE AND SOFTWARE SECURITY

- **Protection Requirements**

This section addresses the objectives for hardware and software security features and assurances.

ISSUES AND HINTS:

- There should be a balance of hardware and software security features, along with other measures (physical, administrative, personnel, and telecommunications)

REFERENCE: *DOE 5637.1, Chapter III, 5a*

- **Determination of Protection Requirements**

ISSUES AND HINTS:

- Measures taken are dependent on the processing situation of the ADP system.
- The Protection Index will be zero if:
  * User clearance is equal to or greater than the level of data on the system,
  * All users have a common need-to-know for all data.
  * A protection index of zero requires that (a) the system has user identification and authentication features, and (b) the system includes physical, personnel, telecommunication, and administrative controls appropriate to the level of data on the system.
- The Protection Index will be one if:
  * User clearance is equal to or greater than the level of data on the system,
  * All users do *not* have a common need-to-know for all data.
  * A protection index of one requires that (a) the system includes all the same protection requirements as for a Protection Index of 0, and (b) the system includes access controls and audit trails.
- The Protection Index will be two if:
  * User clearances are one level below the level of data on the system,
  * A protection index of two requires that (a) the system includes all the same protection requirements as for a Protection Index of 1, and (b) the system includes internal labeling of data.

- The Protection Index will be three if:
  - * User clearances are two levels below the level of data on the system,
  - * A protection index of two requires that (a) the system includes all the same protection requirements as for a Protection Index of 2, and (b) the system includes assurance testing.
- Systems with a protection index greater than one should always have a separate ADP Security Plan.

REFERENCE: *DOE 5637.1, Chapter III, 5.b*

- **Features and Assurances**

Describe the specific protection measures to be employed, or equivalent protections, in the local processing situation and local circumstances. Proof of protection features and assurances is required if the system is not on the Evaluated Products List (EPL) produced by the National Center for Computer Security.

REFERENCE: *DOE 5637.1, Chapter III, 5.c(1); DoD 5200.28-STD*

Access Controls

ISSUES AND HINTS:

- All components of the computing resource must have access control measures to ensure that access is limited to those requiring access.
- The operating system of the ADP system should be designed to prevent unauthorized access to system-level resources.
- List procedures that limit access to system-level resources
- Determine if computer security features that are installed and activated operate as designed.
- Determine if the system permits unauthorized downgrading of a classified file.
- Consider how the separation of multiple classifications of data on the system, and access to that data, are provided by (a) technical methods (e.g., software that checks the user's privileges and authorizations before granting access) or (b) administrative methods (e.g., having separate physical drives for different levels of information; periods processing).

- Evaluate the effectiveness of change-control procedures used to minimize the potential for making unauthorized changes to the system.
- Consider how the contents of computer memory and storage media (e.g., central memory, disk, buffers, controller) are protected against scavenging (e.g., are erased or overwritten) before allowing read access.
- Consider the adequacy of security procedures for the development of software or the introduction of purchased software.
- Describe the procedures in moderate detail or reference a document that contains the detail.

REFERENCE: *DOE 5637.1, Chapter III, 5.c(1)*

Assurance Testing

Basis for Assurance Testing:

ISSUES AND HINTS:

- The ADP Security Plan is the sole basis for determining if the system correctly implements the Classified Computer Security Program.
- All security features described in the Security Plan must be tested to ensure that the specific security requirements have been implemented.
- Consider including known or planned test procedures.

REFERENCE: *DOE 5637.1, Chapter III, 5.c(3)(a)*

Examination of Hardware and Software:

ISSUES AND HINTS:

- There must be reviews of all hardware and software developed by uncleared personnel (before it is placed into use).
- Reviews should be commensurate with the level and sensitivity of the data on the system.

- Reviews are intended to detect features affecting system security.
- Describe the procedures in moderate detail or reference a document that contains the detail.

REFERENCE: *DOE 5637.1, Chapter III, 5.c(3)(b)*

Applications Software

ISSUES AND HINTS:

- Applications cannot be processed or run on the system until their sensitivity level has been considered.
- The applications software owner shall define the security requirements of the software.
- Computer security criteria must be incorporated into the design and test/evaluation review of new or significantly changed computer applications software.
- Computer security reviews must be conducted and documented during the applications design phase.
- Computer security reviews must be conducted and documented during the applications test and evaluation phases.
- The applications programs must be certified by the CSSO.
- Describe the procedures in moderate detail or reference a document that contains the detail.

REFERENCE: *DOE 5637.1, Chapter III, 5.c(4)*

Data Base Management Access Controls.

ISSUES AND HINTS:

- Discuss security protections and access controls of any data base software.
- Describe how the data base manager enforces security, e.g., sets parameters, tracks improper access attempts.

REFERENCE: *DOE 5637, Chapter III, 5.c(5)*

D. ADMINISTRATIVE SECURITY FOR MULTIUSER ADP SYSTEM

A multiuser system is one in which two or more users simultaneously share resources or there is sequential use of resources without assurance of complete sanitation between users.

ISSUES AND HINTS:

- Access to classified information must be restricted to those individuals having proper clearance and need-to-know.
- Describe methods used to prevent unauthorized personnel from accessing classified system components.
- Access control measures must include user identification, authentication, authorization, and accountability.

REFERENCE: *DOE 5637.1, Chapter II, 4.b*

- **User IDs**

  ISSUES AND HINTS:

  - There should be IDs for non-employees (e.g., vendors, contractors).
  - Consider forgery potential during requests for ID assignments.
  - There must be a unique identification of each user.
  - No two users may have the same ID at the same time.
  - Group IDs must be based on unique user IDs.
  - There must be different IDs in different systems/nets at the same site.
  - A record of ID assignment must be kept for three years after user access is terminated.
  - Describe the ID assignment procedures in moderate detail or reference a document that contains the detail.

  REFERENCE: *DOE 5637.1, Chapter III, 4.b(1)*

- **Authentication** (verification of claimed identity).

  ISSUES AND HINTS:

  - Users must be identified and authenticated as part of the process of accessing (e.g., logging onto) the system.

- If passwords are used as the primary means of user authentication, the passwords must be generated and managed in accordance with DOE orders:
  - Passwords must be machine generated.
  - The password generation algorithm must be described.
  - Describe password length and transmission.
  - Describe the methods used to protect password files stored on the ADP system.
  - Passwords protecting classified information must be protected commensurate with the level and category of the information to which they allow access.
- There must be procedures for distributing and protecting authentication materials.
- Authentication must be performed during the first attempt to access the system.
- Logon:
  - The logon attempt rate should be controlled by the system.
  - A maximum of five unsuccessful attempts to access the system should be allowed.
  - The operator or CSSO should be immediately notified when the maximum allowable number of unsuccessful logon attempts is exceeded.
  - The user should be notified at successful logon of (a) the date and time of the last successful logon, and (b) if possible, the number of unsuccessful logon attempts since the last successful logon.
  - Users must be identified and authenticated as part of the process of accessing (e.g., log onto) the system.
  - Describe the procedures in moderate detail or reference a document that contains the detail.

REFERENCE: *DOE 5637.1, Chapter III, 4.b(3); Attachment III-2*

- **Authorization**

ISSUES AND HINTS:
(Applies to system authorization [user accounts] and authorization to access classified files)

- Each file must have an identifiable owner.
- File authorization can be via passwords or access control lists.

REFERENCE: *DOE 5637.1, Chapter III, 4.b(4)*

- **Accountability** (Audit Trail)

ISSUES AND HINTS:

- A monitoring and auditing policy must address misuse, abuse, unauthorized access, and other unusual activity on a system.
- Audit trails should be designed and used to support a damage assessment in the event evidence of a compromise is discovered.
- Accountability information must be collected and periodically reviewed for the purpose of detecting unauthorized access attempts or unusual activity on the system.
- Records of all unusual activity should be retained for a defined period of time.
- The criteria for routine audit analysis should be documented.
- Audit trails must be provided where systems are used to selectively declassify or downgrade files.
- Events causing an entry in the audit trail include at least: successful logons, unsuccessful logon attempts, use of an authentication changing procedure, the blocking of a user ID, the reason for the blocking, and changing the classification or protection level of information.
- Each entry to the audit trail should include: date and time of the event, type of event, ID for unsuccessful or successful logons, or for other events, and the origin of the event.
- Audit trail records must be protected from unauthorized access.
- Consider audit trail accountability in relation to: floppy disks, magnetic tapes (including PCs), removable disks, printer ribbons, memory circuits, boards containing microcode, spare parts, and inventory items.
- Describing the procedures in moderate detail or reference a document that contains the detail.

REFERENCE: *DOE 5637.1, Chapter III, 4.b(5)*

4. PROTECTING UNCLASSIFIED COMPUTER SYSTEMS THROUGH THE PERSPECTIVE OF CLASSIFIED REQUIREMENTS

The guidelines presented in the previous chapter focus on classified ADP systems because Directorate 5200 is concerned that existing systems, and future systems, may become classified. Currently, however, the ADPs that 5200 has developed are unclassified. This chapter discusses the implemention of security features into new systems that (a) will meet the current regulations for unclassified computer systems as defined in DOE Order 1360.2A, "Computer Security Program for Unclassified Computer Systems" and (b) can easily, and at minimal cost, be upgraded to a classified system, if necessary.

DOE Order 1360.2A declares

> *... that DOE computer systems and sensitive unclassified information be protected from improper use, alteration, manipulation, or unauthorized disclosure as a result of criminal, fraudulent, or other improper actions. This Order establishes policy and defines responsibilities for the development and implementation of a DOE-wide computer protection program for DOE computer systems operated for DOE or its contractors ...*

Specifics of the protection program, however, are not spelled out in detail in DOE Order 1360.2A, as they are in DOE Order 5637.1. Security for each unclassified system should be determined on an individual basis by reviewing (a) the narrative description of the system, (b) the statement of threat, (c) the ADP computer security environment description, and (d) the risk assessment. A security plan must always be prepared by the site for any system that contains sensitive or private information.

Although it is not necessary for an unclassified system to fulfill all the security requirements that pertain to a classified ADP, it is recommended that the issues and hints in Section 3.2 of this document be heeded, whenever possible. Doing so will ensure that the existing system not only is secure, but is also prepared for an upgrade to a classified system, if necessary. Also keep in mind that site personnel who must obtain certification and accreditation for the system are completely dependent on your development procedures and documentation.

Below are suggestions for designing security into unclassified ADP security systems. Please remember that these ideas are to help you develop a secure computer system and are not intended to be all-inclusive. Creative solutions to integrating security into a system are always encouraged.

4.1 Determining the Protection Requirements

As mentioned in Section 2.2., the DOE declares what the protection requirements are for a classified ADP system by determining its Protection Index. Although the Protection Index is a feature of a classified security system, determining the Protection Index for an unclassified system is valuable. The Index provides a frame of reference for deciding what security features should be implemented on the unclassified system.

In the past, protection requirements for existing systems developed by Directorate 5200 were tailored to each individual (and often differing) situation. However, all security systems developed up to the present time have the following elements in common:

- The systems have been placed in DOE user-cleared secure areas.
- The systems are unclassified.
- Users are personnel with varying degrees of need-to-know, ranging from the CSSO to maintenance personnel.

As described in Section 2.2, a Protection Index of 1 indicates the following:

- User clearance is equal to or greater than the level of data on the system.
- The systems are multi-user systems.
- Users do not have the same need-to-know status.

Therefore, based on this description and discussions held among security personnel, it is our opinion that the security systems developed by Directorate 5200 should be considered to have a Protection Index of 1.

According to DOE Order 5637.1, the protection requirements of such a system are as follows:

- User identification and authentication features
- Physical controls
- Telecommunications controls
- Personnel controls
- Administrative controls
- Access controls
- Audit trails

4.2 Specific Protection Measures

In this section, security goals and specific actions are proposed for an unclassified system with a Protection Index of 1. Although each system must be judged on an individual basis, we recommend that the elements detailed below be considered in any security system currently being developed under Directorate 5200.

Of the seven security measures listed in Section 4.1, only personnel security is not discussed here. Personnel security is considered the sole responsibility of the site. User identification and authorization, access controls, and audit trails are discussed in Section 4.2.4, Administrative Security.

Hardware and software security is discussed here (Section 4.2.3). Although this element is not specifically required with a Protection Index of 1, attention to this element should be considered, particularly with the possibility of a future change to classified status.

4.2.1 PHYSICAL SECURITY

Goal: To protect access to the facility in which the ADP system resides.

Solution: By reviewing (a) the Narrative Description of the System, (b) the Local Statement of Threat, and (c) the Site Statement of Threat, the designer can become familiar with the physical security measures in force at the site, and use this information to determine what security measures should be pursued with respect to the other baseline security elements.

Note: In general, physical security is the site's responsibility and usually does not affect our existing systems because they have been installed in a secure facility.

Physical security also specifies that the system must be completely separate (physically and logically) from all other systems unless managed under a single ADP Security Plan. Existing systems are standalone systems, which satisfy this requirement.

4.2.2 TELECOMMUNICATIONS SECURITY

Goal: To protect the communications resources and transmission of data, to reduce RF emanations from the system, and to provide cost-effective telecommunications that will be compatible with a system upgrade.

Solution: The telecommunications hardware in current use for the unclassified systems is adequate, i.e., a PDS system is not necessary, nor is fiber optic cabling. However, additional telecommunications security options that can be achieved at low cost are the following:

- *Encryption* protects the confidentiality of information. The National Bureau of Standards adopted the Data Encryption Standard (DES) algorithm as the federal standard in 1977. The DES is inexpensive and can be implemented in either hardware or software. Of the two, the hardware implementation is more efficient. It is also more secure, because integrity of the device can be enhanced by sealing.

  Caution: The latest DOE ruling is that DES can be used only for need-to-know protection, and so it may not be useful for classified processing.

- If encryption is being considered for a classified system, it must be NSA-approved. NSA equipment is more expensive, but it is also more rigorous and secure.

- *Paper seals* around connections can be used to indicate a tamper once it has occurred.

- TEMPEST-proof equipment can be used.

Note: If a Local Area Network (LAN) is being considered for a system, please refer to W. H. Rahe et al., *SNLA Network Security Policy,* SAND88-1705, Sandia National Laboratories, Albuquerque, August 1988. The focus of the document is to provide technical and administrative security information as it pertains to networking.

Also, please be aware that if you are using a LAN for an unclassified system, and the system is upgraded to classified, the LAN must be entirely re-evaluated in terms of the new security requirements.

4.2.3 HARDWARE AND SOFTWARE SECURITY

Goal: To provide the required protection for data processed, stored, transferred, or accessed via the ADP system by implementing a combination of hardware and software security features and assurances, and to prevent unauthorized access to sensitive parts of the system.

Solution: This element is not specifically required for a system with a Protection Index of 1, because it is believed that a balanced combination of the other baseline security elements will provide adequate protection. However, see "Note" below for measures that might be considered.

Note: Some features can be built into a system for protection, particularly if the system may become classified at a later date:

Hardware:

- Separate user data in memory by employing a field length registry.
- Install paper seals at connections to indicate tampering.
- Ideally, cabinets or racks should be designed using one-piece molded metal with as few doors as possible. Such a cabinet ensures that tamper switches and monitors can be added, at low cost, should the system become classified.
- Implement monitor/user modes in hardware.
- Employ hardware partitioning.

Software:

- Software engineering techniques should be followed throughout software development. The documentation prepared as part of the software engineering methodology will be invaluable for developing a security plan.
- Software should be designed to incorporate periodic (automatic and manually invoked) integrity checks of the executing software.
- Write secure software that can be examined for security problems. Produce clear code that behaves in a controlled manner, is easily maintained, and is not vulnerable to security problems. When possible, heed the following guidelines:*
  - Consider security issues when writing code.
  - Partition the system in a modular way that allows changes.

* Gail Barlich, "Some Thoughts on Writing Secure Software," Los Alamos National Laboratory, Los Alamos, NM. (To be published.)

  - Include extensive error recovery procedures, such as (a) requiring confirmation before a user can perform a potentially disastrous action, (b) disabling control characters, and (c) preventing input buffer overflow.
  - Use and enforce a coding standard.
  - Faithfully maintain design documentation and code headers during development.
  - Make sure that someone on the programming staff knows the weaknesses and strengths of your language(s) and operating system. The code should be checked for places where the language's inherent weakness is left for someone to exploit.
  - Avoid rigid coding practices. Don't hard-code the names of data files or "magic" numbers. Use include files of constants so that changes can be made in one place without adversely affecting the program as a whole.
- Design the system so that software does not have to be recompiled after modifications, e.g., use a database rather than block data.
- Partition the hard disk so that you can separate files that are sensitive from other files on the hard disk.
- Store the source code away from the system in a secure area or vault to protect it from unauthorized modifications.
- Protect executable files against unauthorized write, execute, read, and delete.

4.2.4 ADMINISTRATIVE SECURITY

Goal: To provide adequate administrative controls for access to and appropriate handling of information.

Solution: Restrict access to data stored in an ADP system through access control measures, including (a) user identification, (b) authentication, (c) authorization, and (d) accountability.

- User identification and authentication go hand in hand. A unique name and password should be given to each user to enter during the logging on procedure. A group ID can also be assigned. The group ID protects files by assigning read, write, execute, and delete privileges for the group. Follow the identification and authentication guidelines detailed in "Administrative Security for a Multiuser System," Section D of 3.2.5, "Basis for Certification."

- Consider using hardware-based access control systems. Examples of such systems include (a) requiring the user to enter a password on a PC before it will boot up (PC only), and (b) using an ID card reader during the logging on procedure for authentication.

- Provide file authorization by assigning a unique user ID to each user, or through passwords or access control lists. The read, write, execute, or delete privileges can be defined through either construct.

- Provide for accountability with an audit trail. The audit trail should monitor and record any misuse, abuse, unauthorized access, and other unusual activity on the system. Each transaction should be traceable to the individual who entered it. In existing systems, the audit trail software package and the hardcopy logger provide adequate accountability.

- Use automated techniques to analyze audit trail information.

- Consider including an independent process to report any anomalies found in the audit trail.

- Consider providing captive accounts for particular groups of personnel, e.g., maintenance personnel, guards.

- Address how and when security seals will be inspected for tampering.

Note: All of the solutions mentioned above can be achieved with a software package or a comprehensive operating system. Also, the DOE Center for Computer Security is currently developing tools to achieve Administrative Security, and these tools provide many of the above features. For more information, contact the center.

When considering implementing administrative controls into the system, follow the issues and hints in "Administrative Security for a Multiuser System," Section D of 3.2.5, "Basis for Certification."

5. SUMMARY

Since the "Computer Security Act of 1987" became law in January 1988, computer security has become a more prominent national concern. Although security has always been an important consideration for the systems developed by Directorate 5200, it was approached on an informal basis because these unclassified systems were being installed in secure sites.

In light of the new law, however, a more formal approach should be considered for computer-based security systems. This approach is based on the ADP Security Program that is outlined in DOE Order 5637.1, "Classified Computer Security Program." Designers of security systems should be familiar with this policy, so that they can integrate protection into an ADP security system at an early stage.

According to the author and other security personnel, the Protection Index for the current security systems, which are unclassified, is considered to be 1. This index requires seven specific security measures:

- User identification and authentication features
- Physical controls
- Telecommunications controls
- Personnel controls
- Administrative controls
- Access controls
- Audit trails

Of special interest to the security system designer are the security regulations regarding telecommunications and administrative controls, such as user identification features, authentication features, and audit trails. Issues and hints about these security measures, taken from the *Guide to the ADP Security Plans*, have been presented, along with specific protection measures for an unclassified security system. Directorate 5200's systems are usually placed at an outside site, and a cooperative security effort between the site and the designer is desired.

Although current security systems are unclassified, existing or future systems may be reclassified. Therefore, to produce a secure computer system and to prepare for a possible upgrade to classified, it is highly recommended that the issues brought out by DOE Order 5637.1 be considered in the development of any system, classified or unclassified.

APPENDIX A

Glossary

ACCESS CONTROL. The process of limiting access to information or resources on an ADP system to only authorized users.

ACCESS CONTROL MEASURES. Hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these designed to detect or prevent unauthorized access to an ADP system and to enforce access control.

ACCOUNTABILITY. The property that enables activities on an ADP system to be traced to individuals who can then be held responsible for their activities.

ACCOUNTABILITY INFORMATION. A set of records, often referred to as an audit trail, that collectively provide documentary evidence of the processing or other actions related to the security of an ADP system.

ADMINISTRATIVE SECURITY. The management procedures and constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for classified information.

ADP FACILITY. One or more rooms, generally contiguous, containing the elements of an ADP system.

ADP SYSTEM. An assembly of components of computer hardware, telecommunications, interconnections with other ADP equipment (e.g., networks), and the entire collection of software that is executed on that hardware. Included in this definition are word processors, microprocessors, personal computers, controllers, Automated Office Support Systems (AOSS), memory typewriters, and other stand-alone or special computer systems.

ASSURANCE TESTING. A process used to determine that the security features of a system are implemented as designed, and that they are adequate for the proposed environment. This process may include hands-on functional testing, penetration testing, and/or verification.

AUTHENTICATION. The act of verifying the claimed identity of an individual, station, or originator.

AUTHORIZATION. The privilege granted to an individual by a designated official to access information based upon the individual's clearance and need-to-know.

CLASSIFIED COMPUTER SECURITY PROGRAM. All of the technological safeguards and managerial procedures established and applied to ADP Facilities and ADP systems (including computer hardware, software, and data) in order to ensure the protection of classified information.

CLASSIFIED DATA/CLASSIFIED INFORMATION. Top Secret, Secret, and Confidential information of all categories (e.g., RD, FRD, NSI), including intelligence information, for which the DOE is responsible and requires safeguarding in the interest of national security and defense.

COMPROMISING EMANATIONS (TEMPEST). Unintentional data-related or intelligence-bearing signals, which, if intercepted and analyzed, disclose classified information being transmitted, received, handled, or otherwise processed by any information processing equipment.

COMPUTER SYSTEM SECURITY OFFICER (CSSO). Person responsible for preparing the ADP Security Plan consistent with an analysis of the security requirements for the protection of classified information in the classified ADP system and facility.

INFORMATION. The terms "data," "information," "material," "documents," and "matter" are considered synonymous and used interchangeably in this Order. They refer to all data regardless of its physical form (e.g., data on paper printouts, tapes, disks, or disk packs, in memory chips, in Random Access Memory (RAM), in Read Only Memory (ROM), on microfilm or microfiche, on communication lines, and on display terminals).

NETWORK. A communications medium and all components attached to that medium that are responsible for the transfer of information. Such components may include ADP systems, packet switches, telecommunications controllers, key distribution centers, technical control devices, and other networks.

PASSWORD. A protected word, phrase, or a string of symbols that is used to authenticate the identity of a user.

PERSONNEL SECURITY. The procedures established to ensure that all personnel who have access to any classified information have the required authorizations, as well as the appropriate clearances.

PHYSICAL SECURITY.

(a) The use of locks, guards, badges, alarms, procedures, and similar measures (alone or in combination) to control access to the classified ADP system and related equipment.

(b) The measures required for the protection of the structures housing the classified ADP system, related equipment, and their contents from espionage, theft, waste, fraud, abuse, or damage by accident, fire, and environmental hazards.

PROTECT AS RESTRICTED DATA (PARD). The PARD designation is a handling method for computer-generated numerical data, or related information, which is not readily recognized as classified or unclassified because of the high volume of output and low density of potentially classified data. Such information is designated as PARD because it has not had a sensitivity (classification) review and must be protected under a different set of security rules.

PROTECTED DISTRIBUTION SYSTEM (PDS). A telecommunications system to which acoustical, electrical, electromagnetic, and physical safeguards have been applied to permit its use for secure electrical or optical transmission of unencrypted classified information or sensitive unclassified information.

PROTECTION INDEX. A measure of perceived risk determined from the combination of the clearance level of users and the classification of the data on the classified ADP system.

RISK ASSESSMENT. An identification of a specific ADP facility's assets, the threats to those assets, and the ADP facility's vulnerability to those threats.

SECURITY AREA. A physically defined space containing classified matter (documents or material) subject to physical protection and personnel access controls. For further information, consult DOE Order 5632.4.

SITE. One or more operational facilities, usually geographically contiguous, operated by or for the DOE under the management and administrative direction of a DOE or DOE contractor organization.

TEMPEST. An unclassified name referring to the investigation and study of compromising emanations. It is sometimes used synonymously for the term "compromising emanations," (e.g., TEMPEST test and TEMPEST inspections).

USER. Any individual who is able to (a) operate any equipment, (b) implement a procedure that can access the ADP system, (c) input commands to the ADP system, or (d) receive output from the ADP system, without intervention of an authorized reviewing official. Note that a user may not necessarily be an *authorized* user of the ADP system.

APPENDIX B

Additional Sources of Information (Documentation and Personnel)

DOCUMENTATION

CSC-STD-002-85, "Department of Defense Password Management Guideline," of 4-12-85, which provides guidance related to the design, implementation and use of password-based user authentication mechanisms.

DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," of 12-26-85, which defines the classes of computer security protection and provides a basis for the evaluation of effectiveness of security controls built into ADP systems.

DOE 1360.2A, Computer Security Program for Unclassified Computer Systems, of 3-9-79, which establishes policy for safeguarding DOE ADP systems and, in particular, DOE sensitive unclassified information.

DOE 5300.1A, Telecommunications, of 11-16-81, which establishes policy and general guidance for the use, review, coordination, and provision of telecommunications services for the Department of Energy.

DOE 5300.2B, Telecommunications: Emission Security (Tempest), of 5-22-86, which establishes the Department of Energy telecommunications program for emission security.

DOE 5300.3B, Telecommunications: Communications Security, of 2-12-87, which establishes policy, responsibilities, and guidance concerning the communications security (COMSEC) aspects of telecommunications services of the Department of Energy, and implements the national telecommunications protection policy.

DOE 5637.1, Classified Computer Security Program, of 1-29-88, which establishes uniform requirements, policies, responsibilities, and procedures for the development and implementation of a DOE Classified Computer Security Program to ensure the security of classified information in ADP systems.

National Bureau of Standards (NBS) Publications List 91, "Computer Security Publications," of 2-85, which provides a comprehensive listing of all NBS Federal Information Processing Standards, Guidelines, and Special Publications related to the field of computer security.

Public Law 100-235, "Computer Security Act of 1987," which provides for a computer standards program within the National Bureau of Standards, to provide for government-wide security and to provide for the training in security matters of persons who are involved in the management, operation, and use of federal computer systems, and for other purposes.

W. H. Rahe, L. L. Fine, R. M. Jansma, and R. G. Hawkins, *SNLA Network Security Policy,* SAND88-1705. Sandia National Laboratories, Albuquerque, August 1988. The focus of the document is to provide technical and administrative security information as it pertains to networking.

PERSONNEL

Division 2612, Computer Security Division, SNLA.

Division 2645, Network Architecture Functional Design, SNLA.

DOE Center for Computer Security, Los Alamos National Laboratories, Los Alamos, NM.

DISTRIBUTION:

DOE Headquarters

T. E. Wade, Acting Asst. Secy.
Defense Programs
U.S. Department of Energy
DP-1
Washington, DC 20585

W. L. Barker
Defense Programs
U.S. Department of Energy
DP-3
Washington, DC 20585

E. J. McCallum Director
Office of Security Evaluation
U.S. Department of Energy
DP-4
Washington, DC 20545

Dep. Asst. Secy.
Nuclear Materials
U.S. Department of Energy
DP-10
Washington, DC 20585

BG Paul Kavanaugh
Actg. Dep. Asst. Secy.
Military Applications
U.S. Department of Energy
DP-20
Washington, DC 20585

Lew Newby, Director
Weapon Safety & Operations
Office of Military Application
U.S. Department of Energy
DP-22
Washington, DC 20545

Robert K. Peterson
Office of Military Applications
U.S. Department of Energy
DP-222
Washington, DC 20545

Bill Shepard
Office of Military Applications
U.S. Department of Energy
DP-222
Washington, DC 20545

F. C. Gilbert, Acting
Dep. Asst. Secy. for Security Affairs
U.S. Department of Energy
DP-30
Washington, DC 20585

Director of Classification
U.S. Department of Energy
DP-32
Washington, DC 20585

A. Bryan Siebert
U.S. Department of Energy
DP-33
Washington, DC 20585

Elizabeth Q. Ten Eyck, Director
Office of Safeguards and Security
U.S. Department of Energy
DP-34
Washington, DC 20545

O. B. Johnson
Deputy Director
Office of Safeguards & Security
U.S. Department of Energy
DP-34.1
Washington, DC 20545

Director
Division of Policy & Program Support
Office of Safeguards and Security
U.S. Department of Energy
DP-341
Washington, DC 20545

Tom Cousins
Office of Safeguards and Security
U.S. Department of Energy
DP-341.3
Washington, DC 20545

Glenn Hammond, Director
Division of Safeguards
Office of Safeguards and Security
U.S. Department of Energy
DP-342
Washington, DC 20545

K. Sanders, Chief
International Support Branch
Office of Safeguards and Security
U.S. Department of Energy
DP-342.2
Washington, DC 20545

James Branscome
Office of Safeguards and Security
U.S. Department of Energy
DP-342.3
Washington, DC 20545

Richard Peavy, Chief
Technical Development Branch
Office of Safeguards and Security
U.S. Department of Energy
DP-342.3
Washington, DC 20545

David Jones, Director,
Division of Security
Office of Safeguards and Security
U.S. Department of Energy
DP-343
Washington, DC 20545

Chief
Physical Security Branch
Office of Safeguards and Security
U.S. Department of Energy
DP-343.3
Washington, DC 20585

Charles V. Boykin, Acting
Dep. Asst. Secy. for Intelligence
U.S. Department of Energy
DP-40
Washington, DC 20585

John R. Longenecker
Dep. Asst. Secy. for Uranium
Enrichment
U.S. Department of Energy
NE-30
Washington, DC 20545

David J. McGoff
Dep. Asst. Secy. for Reactor
Development
U.S. Department of Energy
NE-50
Washington, DC 20545

Lyle C. Wilcox
Dep. Asst. Secy. for Reactor Systems
Development & Technology
U.S. Department of Energy
NE-50
Washington, DC 20545

David E. Bailey, Director
Division of Fuels & Reprocessing
U.S. Department of Energy
NE-551
Washington, DC 20545

Admiral K. R. McKee
Dep. Asst. Secy. for Naval Reactors
U.S. Department of Energy
NE-60/NR
Washington, DC 20545

Ben C. Rusche, Director
Office of Radioactive Water
Management
U.S. Department of Energy
RW-1
Washington, DC 20585

DOE Field Offices

Director
Safeguards & Security Division
U.S. Department of Energy
Savannah River Operations Office
P.O. Box A
Aiken, SC 29802

W. J. Desmond, Chief
Security Operations Branch
U.S. Department of Energy
Savannah River Operations Office
P.O. Box A
Aiken, SC 29802

J. E. Anderson, Chief
Safeguards & Security Division
U.S. Department of Energy
Savannah River Operations Office
P.O. Box A
Aiken, SC 29802

R. E. Sabre, Director
Transportation Safeguards Division
U.S. Department of Energy
Albuquerque Operations Office
P.O. Box 5400
Albuquerque, NM 87115

George Carnahan
U.S. Department of Energy
Sandia Area Office
P.O. Box 5400
Albuquerque, NM 87115

T. C. Miskowicz, Director
Security Division
U.S. Department of Energy
Albuquerque Operations Office
P.O. Box 5400
Albuquerque, NM 87115

Ray W. Surface, Chief
Inspection & Tech. Sec. Branch
Security Division
U.S. Department of Energy
Albuquerque Operations Office
P.O. Box 5400
Albuquerque, NM 87115

Jerry Howell, Acting Director
Central Training Academy
U.S. Department of Energy
P.O. Box 18041
Albuquerque, NM 87185

Don Jewell
Central Training Academy
U. S. Department of Energy
P.O. Box 18041
Albuquerque, NM 87185

G. W. Johnson
U.S. Department of Energy
Amarillo Area Office
P.O. Box 30030
Amarillo, TX 79120

Richard Phillips, Chief
Safeguards & Security Management
Branch
U.S. Department of Energy
Amarillo Area Office
P.O. Box 30030
Amarillo, TX 79120

Carlton Bingham
U.S. Department of Energy
Chicago Operations Office
New Brunswick Laboratory
9700 South Cass Avenue
Argonne, IL 60439

H. W. Kelley, Director
Safeguards & Security Division
U.S. Department of Energy
Chicago Operations Office
9800 South Cass Avenue
Argonne, IL 60439

M. W. Thomas, Chief
Security Branch
U.S. Department of Energy
Chicago Operations Office
9800 South Cass Avenue
Argonne, IL 60439

Dennis A. Schurman, Administrator
Western Area Power Administration
U.S. Department of Energy
P.O. Box 3402
Golden, CO 80401

Chief
Safeguards & Security Division
U.S. Department of Energy
Rocky Flats Area Office
P.O. Box 928
Golden, CO 80401

R. S. Bostian, Director
Safeguards & Security Division
U.S. Department of Energy
Idaho Operations Office
785 DOE Place
Idaho Falls, ID 83402

Administrator
Alaska Power Administration
U.S. Department of Energy
P.O. Box 50
Juneau, AK 99802

Roger Teska, Chief
Security Section
U.S. Department of Energy
Kansas City Area Office
P.O. Box 202
Kansas City, MO 64141

E. W. Adams, Director
Safeguards & Security Division
U.S. Department of Energy
Nevada Operations Office
P.O. Box 14100
Las Vegas, NV 89114

Physical & Tech. Security Branch
U.S. Department of Energy
Nevada Operations Office
Attn: Donald L. Clough
Ray Escobedo
P.O. Box 14100
Lass Vegas, NV 89114

Jean McGarry, Acting Chief
Safeguards & Security Division
U.S. Department of Energy
P.O. Box 435
Mercury, NV 89023

Fredda South
U.S. Department of Energy
Dayton Area Office
P.O. Box 66
Miamisburg, OH 45342

Director, Strategic Petroleum Reserve
Project Management Office
U.S. Department of Energy
Security Division
900 Commerce Road East
New Orleans, LA 70123

R. R. Fredlund, Director
Safeguards & Security Division
U.S. Department of Energy
San Francisco Operations Office
1333 Broadway
Oakland, CA 94612

Warren Jue, Chief
Inspection and Evaluation Branch
U.S. Department of Energy
San Francisco Operations Office
1333 Broadway
Oakland, CA 94612

D. J. Cook, Director
Safeguards & Security Division
U.S. Department of Energy
Oak Ridge Operations Office
Oak Ridge, TN 37830

Branch Chief
U.S. Department of Energy
Physical Security
Safeguards & Security Division
Oak Ridge Operations Office
Oak Ridge, TN 37830

Distribution Services
Office of Scientific and Technical
Information
U.S. Department of Energy
P.O. Box 62
Oak Ridge, TN 37831

Robert L. Windus, Security Manager
U.S. Department of Energy
Bonneville Power Administration
P.O. Box 3621
Portland, OR 97208

K. H. Jackson, Director
Safeguards & Security Division
U.S. Department of Energy
Richland Operations Office
P.O. Box 550
Richland, WA 99352

Joe W. Wiley
Operations Security Branch
U.S. Department of Energy
Richland Operations Office
P.O. Box 550
Richland, WA 99352

R. F. Timma, Acting Director
Safeguards & Security Division
U.S. Department of Energy
Schenectady Naval Reactors Office
P.O. Box 1069
Schenectady, NY 12301

Warren C. Sherard, Jr.
U.S. Department of Energy
Pinellas Area Office
P.O. Box 2900
Largo, FL 34649

J. A. Bullian, Director
Safeguards & Security Division
U.S. Department of Energy
Pittsburgh Naval Reactors Office
P.O. Box 109
West Mifflin, PA 15122

DOE Contractors

C. R. Meese, Asst. Superintendent
Project Department
Savannah River Plant
E. I. duPont de Nemours and Company
Aiken, SC 29808-0001

N. R. Chronis, Director
Planning and Controls Division
Wackenhut Services, Inc.
P.O. Box W
Aiken, SC 29802

James Hallihan
Mason & Hanger-Silas Mason
Pantex Plant
P.O. Box 30020
Amarillo, TX 79177

Argonne National Laboratory-East
Attn: J. Maguire
L. Wynveen, R. Perry
9700 South Cass Avenue
Argonne, IL 60439

M. E. Remley
Rocketdyne Division
Rockwell International Corporation
P.O. Box 309
Canoga Park, CA 91304

James M. Miller
Security Supervisor
Westinghouse Materials Company of Ohio
P.O. Box 298704
Cincinnati, OH 45239

Terry Hill
Battelle Columbus Laboratories
505 King Ave.
Columbus, OH 43201-2693

Battelle Columbus Laboratories
Attn: Harley Toy, Homer Faust
505 King Ave.
Columbus, OH 43201

Rocky Flats Plant
North American Space Operations
Attn: W. F. Weston, E. R. Young
P.O. Box 464
Golden, CO 80401

Rocky Flats Plant
Attn: Library (M. Moomey)
P.O. Box 464
Golden, CO 80401

Wackenhut Services, Inc.
800 West Commerce Road
Room 120
Harahan, LA 70123

Charlie Abrams
Argonne National Laboratory-West
P.O. Box 2528
Idaho Falls, ID 83401

Argonne National Laboratory-West
Attn: R. Black
W. P. Keeney
P.O. Box 2528
Idaho Falls, ID 83403-2528

G. E. Denning, Manager
Safeguards & Security Section
Westinghouse Idaho Nuclear Co., Inc.
P.O. Box 4000
Idaho Falls, ID 83403

G. B. Sanford, Manager
Safeguards & Security Section
ENICO
P.O. Box 2800
Idaho Falls, ID 83403

J. W. Maloney, Project Manager
American Protective Services
INEL CF-606
785 DOE Place
Idaho Falls, ID 83402

Dan E. Campbell
Naval Reactor Facility
P.O. Box 2068
Idaho Falls, ID 83401

R. E. Gmitter, Manager
General Electric Nuclear Division
Plant Security
P.O. Box 2908
Largo, FL 34294

Holmes & Narver, Inc.
Attn: Electronics Department
P.O. Box 14340
Las Vegas, NV 89114

Jeffrey Herhold
EG&G Energy Measurements, Inc.
M/S B-92
P.O. Box 1912
Las Vegas, NV 89125

J. S. Hunt
Lawrence Livermore National
Laboratory
University of California
P.O. Box 808
Livermore, CA 94550

Dr. Rokaya Al-Ayat
NSS/Safeguards Program Manager
LLNL
MS L-195
P.O. Box 808
Livermore, CA 94550

Darryl B. Smith
Program Manager, Safeguards
Los Alamos National Laboratory
Q-DO/E550
P.O. Box 1663
Los Alamos, NM 87545

C. A. Robertson, Division Leader
Los Alamos National Laboratory
Operational Safeguards & Security
P.O. Box 1663
Los Alamos, NM 87545

Monsanto Research Corporation
Mound Facility
Attn: P. C. Adams, M. P. Shade
P.O. Box 32
Miamisburg, OH 45342

Monsanto Research Corporation
Attn: K. N. Gardner
M. A. Gibson
C. L. Fellers
P.O. Box 32
Miamisburg, OH 45342

Boeing Petroleum Services
850 South Clearview Parkway
New Orleans, LA 70123

Walk Haydell and Associates
600 Carondolet
New Orleans, LA 70130

G. W. Evans
Martin-Marietta Energy Systems
Y-12 Plant
P.O. Box Y
Oak Ridge, TN 37831

Jim Nations
Oak Ridge Gaseous Diffusion
ORGDP Security Department
Bldg. K-1652, MS-351
P.O. Box P
Oak Ridge, TN 37831

A. K. Yancy
Martin-Marietta Energy Systems
Paducah Gaseous Diffusion Plant
P.O. Box 1410
Paducah, KY 42001

M. Maricotz
Martin-Marietta Energy Systems
Paducah Gaseous Diffusion Plant
P.O. Box 1410
Paducah, KY 42001

R. R. Miller, MS 1112
Martin-Marietta Energy Systems
P.O. Box 628
Piketon, OH 45661

Ted Aichele
Hanford Engineering Development
Laboratory
Security Applications Center
P.O. Box 1970, W/B-1
Richland, WA 99352

Doug Carlisle, Manager
Safeguards & Security
Pacific Northwest Laboratory
P.O. Box 999
Richland, WA 99352

Joe Indusi
TSO
Brookhaven National Laboratory
P.O. Box 155
Upton, NY 11973

L. Runge, G. Schoenen and K. Dahms
Brookhaven National Laboratory
P.O. Box 155
Upton, NY 11973

Other Government Agencies

DCS/Security Police
US Air Force in Europe
APO New York 09012-5001

Chief of Security Police
AF Systems Command
Andrews AFB, DC 20334-5000

William A. Wall
FAA Technical Center
ACT-360, Bldg. 202
Atlantic City Airport, NJ 08405

Defense Intelligence Agency
DIA/DX-7B
Bolling AFB, DC 20301-6734

Defense Intelligence Agency
DIA/OS-2A
Bolling AFB, DC 20301-6734

Defense Intelligence Agency
DIA/DT-2B
Bolling AFB, DC 20301-6734

Chief of Security Police
Alaskan Air Command
Elmendorf AFB, AK 95506-5001

Belvoir Research, Development and
Engineering Center
Attn: STRBE-JI (A. Zushin)
Fort Belvoir, VA 22060-5606

Belvoir Research, Development and
Engineering Center
Attn: STRBE-ZM (J. M. Hale)
Fort Belvoir, VA 22060-5606

Belvoir Research, Development and
Engineering Center
Product Manager
Physical Security Equipment
Attn: AMCPM-PSE
Fort Belvoir, VA 22060-5606

Commander
U.S. Army Troop Support Command
Attn: STRBE-1-POLIC
(M. Jennings)
Fort Belvoir, VA 22060

Commanding General
USAJFKSWCS
SOTIC
Ft. Bragg, NC 28307-5000

Commanding General
1st SOCOM
ODCOPS-Special Projects
Ft. Bragg, NC 28307

Col. William F. Garrison
Dept. of Army
1st Special Forces Operational
Det.-Delta
Fort Bragg, NC 28307-5000

U.S. Army Military Police School
ATZN-MP-TS (Capt. Sander)
Fort McClellan, AL 36205-5030

Glenn M. Bell
National Security Agency
M512
Ft. Meade, MD 20755

Duane Davenport, Chief
Physical Security
NSA
Ft. Meade, MD 20755

Robert D. Dikkers, Leader
Building Security Group
National Bureau of Standards
Gaithersburg, MD 20899

485th EIG/EIELD
Attn: C. Winters
Griffiss AFB, NY 13441

HQ USAF/ESD/TCB
Hanscom AFB, MA 01731

DCS/Security Police
Pacific Air Forces
Hickam AFB, HI 96853-5001

Commander
U. S. Army Engineering Division
Attn: HNDED-ME, Electronic
Technology
P. O. Box 1600
Huntsville, AL 35806

HQ USAF/AFOSP
Attn: Gen. Frank Martin
Kirtland AFB, NM 87117-6001

Director of Plans & Programs (SPP)
Air Force Office of Security Police
Kirtland AFB, NM 87117-5000

Director of Operations (SPO)
Air Force Office of Security Police
Kirtland AFB, NM 87117-5000

Chief of Security Police
Tactical Air Command
Langley AFB, VA 23665-5000

DCS/Security Police
Strategic Air Command
Offutt AFB, NE 68113-5000

John Trout
U.S. Army Corps of Engineers,
MROED-S
215 North 17th Street
Omaha, NE 68102

Chief of Security Police
AF Space Command
Peterson AFB, CO 80914-5001

Naval Civil Engineering Laboratory
Attn: G. Cook L-56
Port Hueneme, CA 93043

Chief of Security Police
Electronic Security Command
San Antonio, TX 78243-5000

DCS/Security Police
Military Airlift Command
Scott AFB, IL 62225-5001

Headquarters, EID/EIELD
Attn: P. Stevens
Tinker AFB, OK 73145-6343

Col. Ken Fore, Chairman
U.S. Department of Defense
DoD Physical Security Action Group
OUSDRE/TWP/SP
The Pentagon
Washington, DC 20301

Central Intelligence Agency
Director, Office of Security
202 Jefferson
Washington, DC 20505

U.S. Arms Control & Disarmament
Agency
Chief
Nuclear Safeguards & Tech Div.
320 21st Street, N.W.
Washington, DC 20451

Raymond Brady, Director
U.S. Nuclear Regulatory Commission
Division of Security
Washington, DC 20555

C. C. Slagle, Manager
Technical Division
U.S. Bureau of Engraving & Printing
Room 303M
14th & C Streets SW
Washington, DC 20228

J. Partlow, Director
U.S. Nuclear Regulatory Commission
Division of Inspection Programs
Washington, DC 20555

Robert Burnett, Director
U.S. Nuclear Regulatory Commission
Division of Safeguards
Mail Stop 881-SSS
Washington, DC 20555

Fred Brandt, Chief
Physical Security Branch
U.S. Department of State
DS/PSD Rm 804, SA6
Washington, DC 20520

John Lechevet
U.S. Department of State
DS/ST/CMP Room 2513
Washington, DC 20520

Mr. Richard J. Solan, Chief
U.S. Secret Service
Security Division/Planning &
Development
1800 G. Street N.W., Room 941
Washington, DC 20223

John C. Hagan
National Aeronautics and Space
Administration
Security Office (NIS)
Washington, DC 20546

James W. Atherton, SA
Federal Bureau of Investigation
Washington Field Office
Washington, DC 20538

Bill Hunteman
Los Alamos National Laboratory
P.O. Box 1663, Mail Stop E-541
Los Alamos, NM 87545

2612	R. M. Jansma
2612	L. L. Fine
2612	W. H. Rahe
2612	B. Stiefeld
3430	R. L. Wilde
5200	J. Jacobs
5210	C. C. Hartwigsen
5212	J. C. Matter
5213	J. T. Risse
5214	W. F. Hartman
5215	L. G. Stotts
5217	D. C. Mangan
5219	R. W. Moya
5220	A. A. Lieber
5221	J. W. Kane
5230	M. L. Kramm
5231	E. R. Julius
5233	D. C. Hanson
5234	C. L. Schuster
5235	J. C. Mitchell
5238	R. C. Beckmann
5240	D. S. Miyoshi
5245	I. G. Waddoups
5245	D. A. Faculjak (15)
5246	R. P. Syler
5248	J. P. Martin
5249	B. J. Steele
5250	T. A. Sellers
5251	E. A. Chipman
5252	M. J. Eaton
5253	R. F. Davis
5255	P. D. Merillat
5256	R. P. Glaser
5260	J. R. Kelsey
5261	J. D. Williams
5265	L. G. Stotts
5267	S. C. Roehrig
5268	S. J. Weissman
7233	R. E. Smith
8233	R. Y. Lee
8233	J. M. Harris
8524	J. A. Wackerly
8536	E. F. Diemer
8536	S. Folkendt
3141	S. A. Landenberger (5)
3151	W. I. Klein (3)
3154-1	For DOE/OSTI (Unlimited Release) (8)