

NEW NIST PUBLICATION

October 1990

U.S. DEPARTMENT OF ENERGY RISK ASSESSMENT METHODOLOGY

Volume I: DOE Risk Assessment Guideline Instructions, Resource Table, and Completed Sample

Volume II: DOE Risk Assessment Worksheets

**Edward Roback
NIST Coordinator**

**U.S. DEPARTMENT OF
COMMERCE
National Institute of
Standards and Technology
Gaithersburg, MD 20899**

**U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary**

**National Institute of Standards and
Technology
John W. Lyons, Director**

NIST

U.S. DEPARTMENT OF ENERGY RISK ASSESSMENT METHODOLOGY

Volume I: DOE Risk Assessment Guideline Instructions, Resource Table, and Completed Sample

Volume II: DOE Risk Assessment Worksheets

**Edward Roback
NIST Coordinator**

**U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and
Technology
Gaithersburg, MD 20899**

MAY 1990



**U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary**

**National Institute of Standards and
Technology
John W. Lyons, Director**

Preface

This National Institute of Standards and Technology Interagency Report (NISTIR) presents a risk assessment methodology developed by the U.S. Department of Energy. This NISTIR contains Volume I: DOE Risk Assessment Guideline Instructions, Resource Table, and Completed Sample and Volume II: DOE Risk Assessment Worksheets. The glossary and bibliography which are referenced in the text follow Volume II. Although there are references to a diskette in the text, no diskette has been reproduced for distribution with this NISTIR.

The National Institute of Standards and Technology (NIST) makes no claim or endorsement of this methodology. However, as this material may be of use to other organizations, the report is being reprinted by NIST to make it publicly available and to provide for broad dissemination of this federally sponsored work. This publication is part of a continuing NIST effort to assist federal agencies in accordance with NIST's mandate under the Computer Security Act of 1987.

NIST expresses its appreciation to the U.S. Department of Energy for their permission to publish this report.

Questions regarding this publication should be addressed to the Associate Director for Computer Security, National Computer Systems Laboratory, Building 225, Room B154, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

Additional copies of this publication may be purchased through the National Technical Information Service, Springfield, VA, 22161, telephone: (703) 487-4650.

DEPARTMENT OF ENERGY



VOLUME I

**DOE RISK ASSESSMENT GUIDELINE INSTRUCTIONS,
RESOURCE TABLE, AND COMPLETED SAMPLE**

-- A Structured Approach --

September, 1989

T A B L E O F C O N T E N T S

Page
Number

VOLUME I: DOE RISK ASSESSMENT INSTRUCTIONS,
RESOURCE TABLES AND COMPLETED SAMPLE
(BIBLIOGRAPHY AND GLOSSARY ON DISKETTES)

INTRODUCTION		1
1.	Background	1
2.	Objectives of the Guideline	2
3.	Organization of the Guideline	3
4.	Description of the Guideline's Mechanics	4
STEP 1	DEFINE YOUR SYSTEM	12
R1.2A	Small/Simple System	17
R1.2B	Large/Complex System	18
R1.3	Software: Types, Uses, Storage Media Software and Data Cost Guidance	20
STEP 2	CHARACTERIZE YOUR SYSTEM, SOFTWARE, AND DATA	22
R2.1	Rating the Importance of a System, Its Software and Data	24
R2.2a	Types and Examples of Sensitive Unclassified Data and Software	26
R2.2b	Types of Classified Data and Software; Modes of Operation	27
STEP 3	REVIEW BASELINE SECURITY REQUIREMENTS (BLSRs) AND IDENTIFY THOSE NOT MET OR PARTIALLY MET	29
R3	Master List of DOE Baseline Security Requirements	34
STEP 4	REVIEW THREATS AND VULNERABILITIES AND IDENTIFY ANY WHICH AFFECT YOUR SYSTEM	37
R4.1	Sample Impacts of Threats to and Vulnerabilities of the Physical Facility	41
R4.2	Sample Impacts of Threats to and Vulnerabilities of Personnel	42
R4.3	Sample Impacts of Threats to and Vulnerabilities of Information, Data, and Emissions	43

T A B L E O F C O N T E N T S
(Continued)

	<u>Page Number</u>
R4.4 Sample Impacts of Threats to and Vulnerabilities of Communications	44
R4.5a Sample Impacts of Threats to and Vulnerabilities of Computer Hardware	45
R4.5b Sample Impacts of Threats to and Vulnerabilities of Computer Software	46
R4.6 Sample Impacts of Threats to and Vulnerabilities of ADP System procedures, Administration and Management	47
R4.7a Environmental Threats: Data on U.S. Earthquake Activity	48
R4.7b Environmental Threats: Data on U.S. Tornado Activity	49
R4.7c Environmental Threats: Data on U.S. Thunderstorm Activity	50
R4.7d Map of DOE Facilities in the U.S.	51
STEP 5 REVIEW AND SELECT COUNTERMEASURES OR ACCEPT CURRENT RISK PROFILE	53
R5.1a Countermeasures Guidance: Physical Security	57
R5.1b Countermeasures Guidance: Personnel Security	58
R5.1c Countermeasures Guidance: Information Security	59
R5.1d Countermeasures Guidance: Communications Security	60
R5.1e Countermeasures Guidance: Emissions Security (TEMPEST)	61
R5.1f Countermeasures Guidance: Computer Security	62
R5.1g Countermeasures Guidance: Administrative/ Procedural Security and Security Management	63

T A B L E O F C O N T E N T S
(Continued)

	<u>Page Number</u>
R5.1h Countermeasures Guidance: Environmental Security and Safety	64
R5.1i Guidance for Determining Costs for Countermeasures	65
STEP 6 OBTAIN ACCOUNTABILITY	66
COMPLETED SAMPLE	
Executive Summary	CS-3
Worksheets	CS-10
ANNOTATED BIBLIOGRAPHY (ON FLOPPY)	
1. Risk Assessment: General	
2. Risk Assessment: Computer Based Tools	
3. Threats and Vulnerabilities	
4. Countermeasures: Equipment and Technologies	
5. Countermeasures: Procedures	
6. Networks	
7. Viruses and Other Related Threats	
8. Risk Management	
9. Certification and Accreditation	
10. Other U.S. Government Computer Security Publications	
GLOSSARY (ON FLOPPY)	

INTRODUCTION

INTRODUCTION

1. BACKGROUND

The DOE Risk Assessment Instructions, Resource Tables, and Completed Sample -- A Structured Approach is the result of a joint program sponsored by the Department of Energy's (DOE) Office of ADP Management (MA-24) and the Computer and Technical Security Branch (DP-343.2). It was developed for the Department under contract by Booz, Allen & Hamilton Inc. The program grew out of a concern shared by both the Unclassified and Classified Computer Security Programs at DOE that the risk assessment process needed to be simplified and streamlined in order to allow ADP managers and end users to quickly understand and accomplish risk assessments in a more effective and expeditious fashion. The Guideline provides DOE with a systematic approach. There is documentation for each step performed as well as Executive Summary pages from which management can make cost-effective decisions on safeguard initiatives.

The need to develop such an approach was given impetus with the publication of OMB Circular A-130, "Management of Federal Information Resources," which placed additional emphasis on conducting risk assessments of all types of Government computer systems. Appendix III of A-130 underscored that such assessments are to provide the basis for making informed management decisions related to accepting identified risks or for implementing appropriate cost-effective countermeasures. It also allowed for varied approaches to fulfill the risk assessment requirement: risk assessments may vary from "an informal review of a microcomputer installation to a formal, fully quantified risk analysis of a large scale computer system."

The Department's 1988 publication of DOE Order 1360.2A, Unclassified Computer Security Program, and DOE Order 5637.1, Classified Computer Security Program, also reflect the need to use the risk assessment process as an effective management tool for properly allocating security resources. In fact, the DOE Unclassified Computer Security Program urges those conducting risk assessments to carefully select the risk assessment approach that is best suited to their particular needs: "When used inappropriately (i.e., selecting an inappropriate methodology just to satisfy a general policy requirement), risk assessments can be costly and ineffective for all involved."* The use of a structured approach can expedite the risk assessment process.

The use of this Risk Assessment Guideline is not mandatory. It has proven to be an effective tool through DOE field tests and will be matured as user experience is gained.

*Department of Energy, "FY 1990 - FY 1994 Information Technology Resources Long Range Plan," p. 5.3-1.

2. OBJECTIVES OF THE GUIDELINE

The concept for the Guideline was developed after a thorough review of current approaches to and views on risk assessment was completed. Security professionals in both Government and commercial circles were interviewed to identify what "worked" and what didn't "work" with respect to risk assessment. Consensus among the interviewees was strong that risk assessment was NOT beneficial if it was:

- . Excessively detailed and lengthy -- making it a paper exercise rather than a beneficial management and security awareness process
- . Overly quantitative in approach, thus resulting in an end-product that is difficult to interpret (if not useless)
- . Not oriented towards the true "bottom-line": "What is it going to cost to fix the problems identified?"

A thorough review of the DOE's computer security culture, environment, and unique ADP applications was also undertaken. Again, views regarding the utility of risk assessment underscored many of the same concerns as were expressed above. Risk assessment had become a paper process divorced from the management decision-making process with which it must be integrated in order to achieve accountability for accepting a system's current risk profile and/or for allocating additional security resources.

Discussions and correspondence with several DOE computer security professionals indicated other areas of the risk assessment process were of concern. There was an indication that it was difficult to determine the scope of a risk assessment and the necessary amount of documentation was undefined. Some aspects of cost evaluation that related to intangible or subjective assets was difficult to perform.

Upon completion of the community wide interviews and DOE survey and review, a set of comprehensive objectives were established for the Guideline. The Guideline should be:

- . Simple to understand and use
- . Generally consistent with and useful for both unclassified and classified environments
- . Cost-effective
- . Self-contained for ease of utilization
- . Appropriate for use by most sites
- . An information source

- . Non-labor or time intensive for the user
- . Capable of providing accountability
- . Adaptable for use/integration with currently used risk assessment methodologies
- . Flexibly structured to permit use of existing computer security documentation as input into the risk assessment framework
- . Useful in providing assessments and recommendations of value to managers responsible for accepting risks or planning and funding computer security improvements.

The approach to conducting risk assessments presented in this Guideline was developed with these objectives firmly in mind. The Guideline's structured approach fully meets the risk assessment requirements imposed on the Department's ADP systems by Federal and Department computer security policy, while eliminating numerous "wheel-spinning" problem areas that have consistently complicated risk assessment efforts in the past.

3. ORGANIZATION OF THE GUIDELINE

The Guideline is organized into two major parts which are divided into two separate volumes. Volume I, the main body of the Guideline includes general introductions and references. Volume I also consists of instructions for Steps 1 through 6 and a completed sample. Also included are a Bibliography, and a Glossary on 5 1/4" floppy diskettes. Volume II consists of the Worksheets for each step for completing the Guideline.

In order to effectively use the Guideline, working copies of Volume II, the Worksheets and Executive Summary, need to be made. Second, as you read Volume I instructions, open Volume II to the appropriate worksheet. The worksheet copies are not included in Volume I. Notice there are individual instructions for the worksheets. A resource table is included with the instructions where appropriate. This organization necessitates that both volumes be open to the same step in the risk assessment process.

Table of Contents are in Volume I. The contents and purpose of each of the Guideline's elements are as follows:

(1) Volume I of the Guideline:

INTRODUCTION: The introduction describes the Guideline's background, its underlying philosophy and objectives, and the mechanics involved in using the Guideline. It also provides general instructions for Guideline use.

- . 6 STEP APPROACH: The 6 steps provide the structured approach for conducting the risk assessment. Each step has a particular area of concern; Worksheets provide the necessary data sets and an organized format to address each of the areas of concern. Exhibit 1 presents an overview of the 6 steps and their main area of concern. It also lists the worksheets and resources tables that are used to support each step. A detailed discussion of how the process works -- its mechanics -- is presented in Section 4 below.
- . COMPLETED SAMPLE: The completed sample illustrates how the worksheets and Executive Summary are to be completed. A description of an ADP system/installation is provided, and then the Guideline's approach is used to conduct a risk assessment of this sample system/installation.
- . ANNOTATED BIBLIOGRAPHY: The annotated bibliography, covering the period 1983 - 1988, consists of ten main topical sections on key areas of concern to those conducting risk assessments, from threat and vulnerability-related articles to literature on specific countermeasures for coping with various types of threats. Special interest sections on viruses and networks are also included. In addition, the bibliography contains references to numerous U.S. Government computer security guidance documents.
- . GLOSSARY: The glossary provides a useful compendium of terms common to the risk assessment process. Three DOE sources were used as a starting point for developing the glossary. These were then edited to suit the needs of the Guideline and additional terms were added to ensure coverage of all key terms mentioned herein.

(2) Volume II of the Guideline:

- . WORKSHEETS: The Worksheets provide the necessary documentation to complete the 6 STEP APPROACH as detailed in Volume I.
- . EXECUTIVE SUMMARY: The Executive Summary is the final worksheet which provides a 6 page set of summary sheets for use in recording the results of each step of the risk assessment, and for obtaining management sign-off for the end-results and any resulting recommendations.

4. DESCRIPTION OF THE GUIDELINE'S MECHANICS

The Guideline provides a systematic, structured approach to the various evaluations and decision making processes that comprise a risk assessment. The intent is to provide an approach that allows you -- whether your system is in an unclassified or classified environment or whether it is a PC on large system -- to readily identify and, wherever possible, have available in one package, all

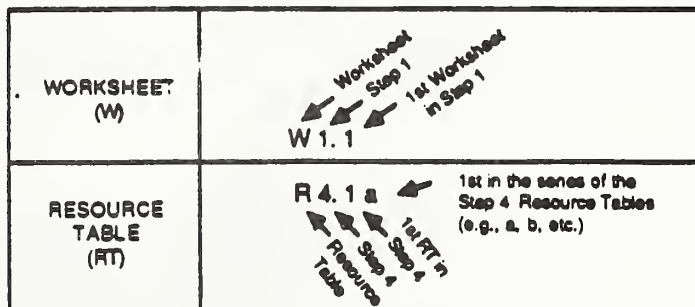
information necessary to conduct a risk assessment. The risk assessment provides for a "short form" and a "long form". The "short form" is adequate for microcomputers, standalone systems, and systems that process unclassified or sensitive information. The "long form" is primarily used for evaluating large systems, systems used primarily for classified processing, and network systems.

Through use of the Guideline, a useful end-product (e.g., the Executive Summary) results. Results are enhanced when the knowledge of security professionals within the organization is used. Further, the structure of the Guideline allows you to go "off-line," if desired, and use a risk assessment tool that has proven useful in the past, and to enter the results of these "off-line" analyses on the appropriate section of the Guideline's Executive Summary. The Guideline can be tailored for use in a specific setting by allowing the assessor to conclude the assessment at the end of Step 3 when further analysis is not deemed necessary. Likewise, the Guideline allows the assessor to complete the Executive Summary, and provide the necessary input for the risk assessment process. Care should be taken while compiling and storing the results of the risk assessment. These results will be sensitive or classified since they address system specific threats and vulnerabilities.

A series of informational Resource Tables accompanies each step. The Worksheets are organized to collect specific types of information needed to support the risk assessment process. Their structure is simple and logical, and they are explained by step-by-step instructions to maximize their utility and minimize wheel-spinning. The Resource Tables provide the majority of data and information necessary to complete the Worksheets for each type of system that is assessed. Data sets, as required, were also tailored to meet DOE-specific requirements.

The contents of Volume II should be copied in its entirety. It contains the Worksheets and Executive Summary sheets. Remember, the guide may be used any number of times and Volume II must be maintained. Also, there is a numbering system to help you quickly identify how the Worksheets and Resource Tables are correlated.

NUMBERING SYSTEM FOR WORKSHEETS AND RESOURCE TABLES



Also, there is a special graphic border in the right hand margin to help identify the Worksheets.

**WORKSHEET
BORDER**



You are also encouraged to draw upon existing documentation to augment the data sets that are provided in the Guideline. Documents of potential use from the Unclassified Computer Security Program include: inventory information developed for the ADP Long Range Plan, the Computer Protection Plan, results of compliance and management reviews, audit reports, incident reports, and certification documentation. Documentation from the Classified Computer Security Program of potential use include: the Statement of Threat, Computer Security Plan, Long Range Plan, System Test and Evaluation results, inspection results, and accreditation documentation. The remainder of this section provides additional detail on each of the 6 steps and their inter-relationship. The overall decision making process involved in using this approach is depicted in the Exhibit 2 at the end of this section.

(1) STEP 1: DEFINE YOUR SYSTEM. The purpose of Step 1 is to produce a general definition of your system by looking at several key system features: composition, connections, size, cost(s), and back-ups. First, the current configuration of your system is established to ensure that you have fully identified all major system components and connections. Use of a system configuration diagram provides you a visual opportunity to record and review your system's current configuration. It also allows you to visualize potential vulnerabilities that may exist as a result of your system's connections and data flows. Second, Step 1 helps you in developing a general cost estimate for your system so that you are able to appreciate how much it would cost to replace it in its entirety. It is also important to have a general appreciation for the cost of your system in order to decide which countermeasures, if any, are justified based on the cost of your system. Step 1 also reviews the type of software and data used by your system, with the objective of understanding approximately how much labor went into the development of each and whether back-ups are available and necessary.

The end products from Step 1 are: (1) A system configuration diagram which depicts your system's major components and connections, (2) a current listing of your system's major components, and (3) rough cost estimates for replacing your system's hardware, software and data.

(2) STEP 2: CHARACTERIZE YOUR SYSTEM, SOFTWARE, AND DATA. The purpose of Step 2 is to characterize your total system in terms of several key characteristics. Questions in two primary areas are answered in this Step: (1) Does your system process any classified information or sensitive unclassified information? If so, what types/levels? Responses to these questions provide the

basis for selecting what type(s) of security precautions are required for your system, software and data; and (2) How important is your system, its operations, software and data to its users and their organization? Responses to this second question will help you determine the relative importance of the system, software, and data, and provide the basis for determining or validating your contingency planning needs.

The end-products produced in Step 2 are: (1) An assessment of the relative importance of your system, software, and data to their users and organization; and (2) an identification of what types of information you are processing (e.g., unclassified, sensitive unclassified, or classified).

(3) STEP 3: REVIEW BASELINE SECURITY REQUIREMENTS (BLSRs) AND IDENTIFY THOSE NOT MET OR PARTIALLY MET. The purpose of Step 3 is to determine whether your system's hardware, software, and data -- as they exist today in their current operating environment and utilized by you and your organization -- meet the minimum Baseline Security Requirements (BLSRs) set forth in all applicable DOE Orders. The Baseline Security Requirements as used in this guideline encompass DOE Orders 1360.2A, 5637.1, and all relevant guidelines, orders, laws, etc. In the previous step you identified whether your system was involved in sensitive unclassified or classified processing. In this step, you are asked to review brief lists of security countermeasures (baseline security requirements) that **MUST** be in place, per the applicable DOE orders.

Step 3 will result in an assessment of your current security profile in terms of: (1) whether you currently have met the DOE's minimum baseline security requirements that apply to sensitive unclassified and classified ADP processing; (2) a list of any noted deficiencies that must be corrected; and (3) target dates for correcting them. It also allows you to note any areas where you desire to supplement the countermeasures currently in-place if you feel it is justified based on Step 1 and Step 2 results.

Further, for the majority of small/simple systems (as defined in Step 1 of this process), the Step 3 results provide an adequate assessment of the current risks to your system. Therefore, Step 3 also documents the decisions made to accept or upgrade your current risk profile, and provides the basis for obtaining management sign-off for these decisions. For these systems, the risk assessment process is complete.

(4) STEP 4: REVIEW THREATS AND VULNERABILITIES AND IDENTIFY ANY WHICH AFFECT YOUR SYSTEM. The purpose of Step 4 is to conduct a more extensive review of the threats that might affect your system's hardware, software and data through exploitation of specific vulnerabilities in your system and its operating environment. In this step, you are asked to record which specific threats could impact your system due to existing deficiencies in your security profile. Further, the Step also

addresses the probability that a given threat could arise at your site or in your locality. (An uncomplicated probability scheme is provided for your use in order to accomplish this.) Finally, the Step also allows you to specify the priority in which the identified threat(s) should be treated.

The end-products that result from Step 4 are: (1) a threat and vulnerability analysis of your system, facility, and its assets within its operating environment. It will also (2) allow you to identify which of the applicable threats are: very likely to occur, likely to occur, or unlikely to occur. Finally, Step 4 will provide the basis for determining which vulnerabilities should be corrected, and in what order, based on the simple probabilities identified for threat occurrence.

(5) STEP 5: REVIEW AND SELECT COUNTERMEASURES OR ACCEPT CURRENT RISK PROFILE. The purpose of Step 5 is two-fold. It provides an opportunity to review available countermeasures in each of the security discipline areas and decide which ones are appropriate for implementation to counter the threat impacts identified in Step 4. However, if your review of the threat impacts does not result in the identification of any new concerns, and confirms that your security program fully treats all possible threat scenarios for your system and site, then Step 5 also allows you to acknowledge this by accepting your current risk profile.

Step 5 results in (1) a prioritized list of countermeasures for implementation in each of the security discipline areas; OR (2) a formal acceptance of your current risk profile made based on a documented review and analysis of possible threat impacts to your system.

(6) STEP 6: OBTAIN ACCOUNTABILITY: MANAGEMENT UNDERSTANDING OF YOUR RISK PROFILE AND COUNTERMEASURES REQUIRED. Step 6 is the last and final step in the risk assessment process. It is a highly critical step, one that is often overlooked or neglected. The purpose of Step 6 is to obtain management accountability for the decisions and choices made throughout the risk assessment process. It provides a mechanism for briefing, reviewing, and discussing the risk assessment results with management and planning resources required for implementing the countermeasures identified.

The Executive Summary Block for Step 6, Obtain Accountability: Management Understanding of Your Risk Profile and Countermeasures Required, provides a sign-off area for management to review the results of the risk assessment, and accept the current risk profile. This sign-off is the final end-product.

It is important to maintain the results of the risk assessment for use in subsequent assessments.

STEPS	AREAS COVERED BY STEP	REQUIRED WORKSHEETS AND RESOURCE TABLES FOR EACH STEP	
		WORKSHEET	RESOURCE TABLE
1 DEFINE YOUR SYSTEM	<ul style="list-style-type: none"> • SYSTEM: <ul style="list-style-type: none"> - CONFIGURATION - CONNECTIONS - SIZE - COST(S) • SOFTWARE AND DATA <ul style="list-style-type: none"> - COSTS - BACK-UPS 	W1.1 SYSTEM COMPOSITION, CONNECTIONS, AND CONFIGURATION W1.2 HARDWARE INVENTORY AND COST W1.3 SOFTWARE INVENTORY AND COST W1.4 DATA INVENTORY AND COST	R1.1 SMALL/SIMPLE SYSTEM <ul style="list-style-type: none"> • DEFINITION • COST GUIDANCE • COMPONENTS R1.2 LARGE/COMPLEX SYSTEM. <ul style="list-style-type: none"> • DEFINITION • COST GUIDANCE • COMPONENTS R1.3 <ul style="list-style-type: none"> • SOFTWARE: TYPES, USES, STORAGE, MEDIA • SOFTWARE AND DATA: COST GUIDANCE
2 CHARACTERIZE YOUR SYSTEM, SOFTWARE, AND DATA	<ul style="list-style-type: none"> • DATA SENSITIVITY OR CLASSIFICATION • NUMBER OF USERS • FREQUENCY OF USE • IMPACT IF UNAVAILABLE 	W2.1 SYSTEM CHARACTERISTICS AND IMPORTANCE W2.2 SOFTWARE CHARACTERISTICS AND IMPORTANCE W2.3 DATA CHARACTERISTICS AND IMPORTANCE	R2.1 RATING THE IMPORTANCE OF A SYSTEM, ITS SOFTWARE AND DATA R2.2a TYPES AND EXAMPLES OF SENSITIVE UNCLASSIFIED DATA AND SOFTWARE R2.2b TYPES OF CLASSIFIED DATA AND SOFTWARE, AND MODES OF OPERATION
3 REVIEW BASELINE SECURITY REQUIREMENTS (BLSRS) AND IDENTIFY THOSE NOT MET OR PARTIALLY MET (IDENTIFY SUPPLEMENTAL UPGRADES IF DESIRED.)	<ul style="list-style-type: none"> • BLSRS BY SECURITY DISCIPLINE: <ul style="list-style-type: none"> - PHYSICAL - PERSONNEL - INFORMATION - COMPUTER - COMMUNICATIONS - EMISSIONS - PROCEDURAL/ADMINISTRATIVE/MANAGEMENT - ENVIRONMENTAL/SAFETY 	REVIEW OF BASELINE SECURITY REQUIREMENTS (BLSRS) FOR W3.1a&b PHYSICAL SECURITY W3.2 PERSONNEL SECURITY W3.3 INFORMATION SECURITY W3.4 COMMUNICATIONS SECURITY (COMSEC) W3.5 EMISSIONS SECURITY (TEMPEST) W3.6a&b COMPUTER SECURITY W3.7 ADMINISTRATIVE/PROCEDURAL SECURITY AND SECURITY MANAGEMENT W3.8a&b ENVIRONMENTAL SECURITY AND SAFETY	R3 MASTER LIST OF DOCUMENTS FOR BASELINE SECURITY REQUIREMENTS (BLSRS)
4 REVIEW THREATS AND VULNERABILITIES AND IDENTIFY ANY WHICH AFFECT YOUR SYSTEM	<ul style="list-style-type: none"> • THREATS AND VULNERABILITIES <ul style="list-style-type: none"> - BY IMPACT: <ul style="list-style-type: none"> • DENIAL • DESTRUCTION • DISCLOSURE • DAMAGE - BY PROBABILITY - BY PRIORITY OF CONCERN 	W4 THREAT AND VULNERABILITY REVIEW	THREAT AND VULNERABILITY GUIDANCE (BY ASSET). R4.1a&b PHYSICAL (FACILITY) R4.2a&b PERSONNEL R4.3a&b INFORMATION, DATA, AND EMISSIONS R4.4a&b COMMUNICATIONS R4.5a-d COMPUTER (HARDWARE AND SOFTWARE) R4.6a&b PROCEDURES, ADMINISTRATION, AND MANAGEMENT R4.7a-d ENVIRONMENTAL
5 REVIEW AND SELECT COUNTERMEASURES OR ACCEPT CURRENT RISK PROFILE	<ul style="list-style-type: none"> • COUNTERMEASURES BY SECURITY DISCIPLINE AND TYPE: <ul style="list-style-type: none"> - EQUIPMENT OR PROCEDURAL - COST - PRIORITY OF FIX - TARGET DATE 	W5 COUNTERMEASURES IDENTIFICATION AND RISK PROFILE ACCEPTANCE	R5.1 COUNTERMEASURES GUIDANCE. R5.1a PHYSICAL SECURITY R5.1b PERSONNEL SECURITY R5.1c INFORMATION SECURITY R5.1d COMMUNICATIONS SECURITY R5.1e EMISSIONS SECURITY (TEMPEST) R5.1f COMPUTER SECURITY R5.1g ADMINISTRATIVE/PROCEDURAL SECURITY AND SECURITY MANAGEMENT R5.1h ENVIRONMENTAL SECURITY AND SAFETY R5.1i GUIDANCE FOR DETERMINING COST(S) OF COUNTERMEASURES
6 OBTAIN MANAGEMENT REVIEW, PARTICIPATION AND ACCOUNTABILITY	<ul style="list-style-type: none"> • ACCEPTANCE OF RISK(S) • COMMENTS/EXCEPTIONS • UPGRADES REQUIRED <ul style="list-style-type: none"> - BUDGET NEEDS - PLAN OF ACTION 	<ul style="list-style-type: none"> • MANAGEMENT BRIEFING DEVELOPED USING THE EXECUTIVE SUMMARY • EXECUTIVE SUMMARY • SUPPORTING DOCUMENTATION 	

EXHIBIT 1
An Overview of the DOE's
Structured Approach to Risk Assessment

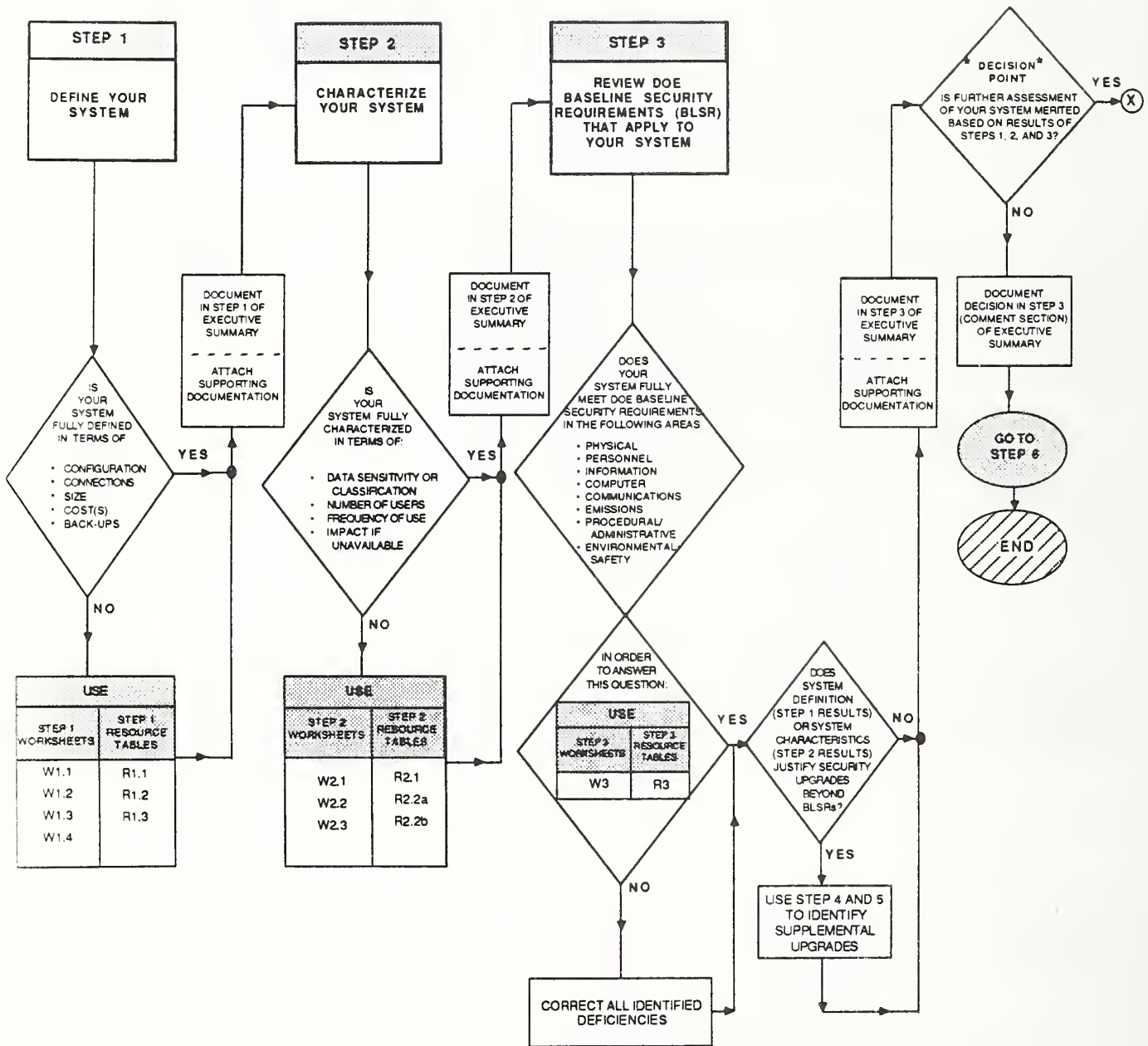


EXHIBIT 2
Decision Flow Diagram Depicting the 6-Step Process
in the DOE Risk Assessment Guideline

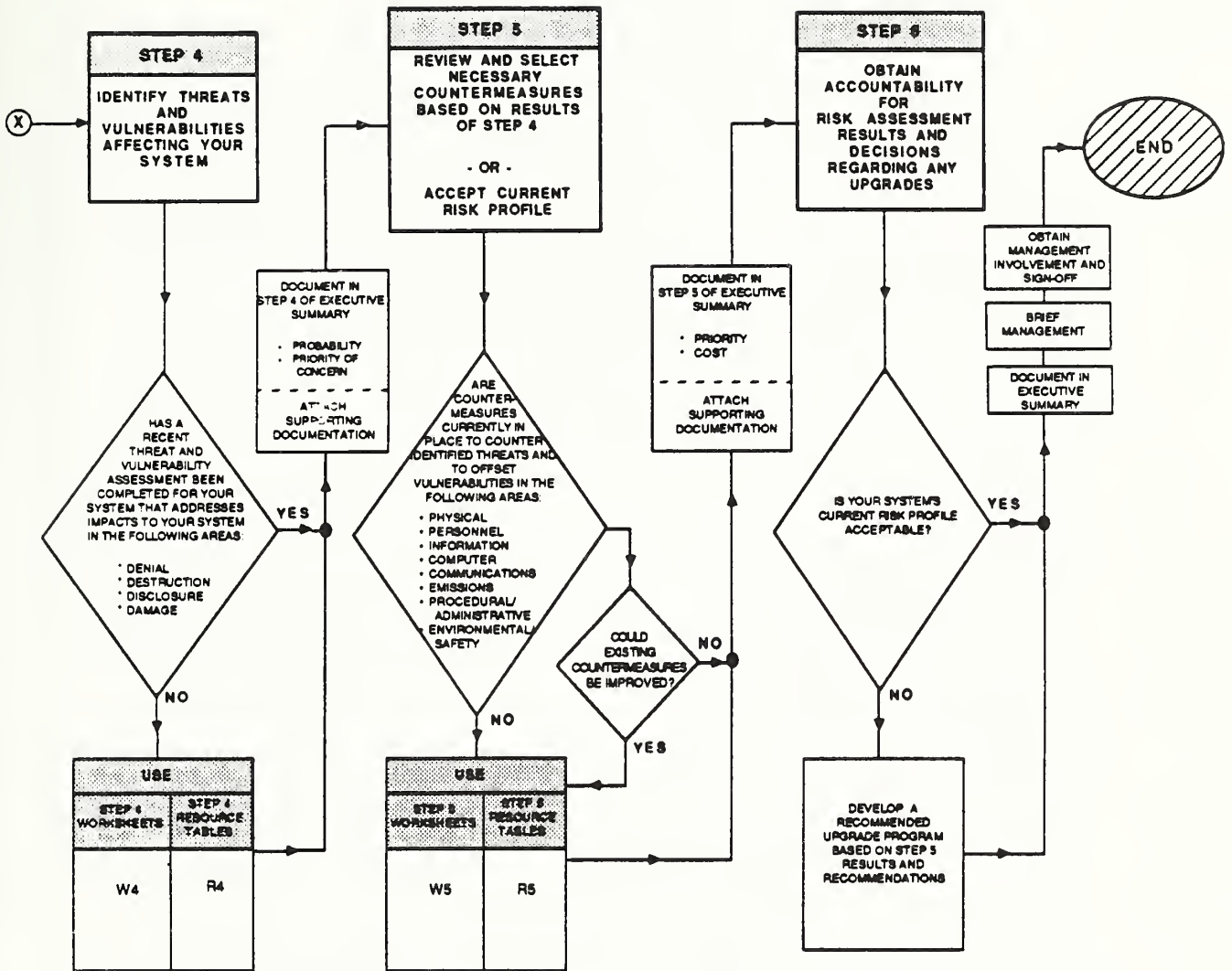


EXHIBIT 2 (CONT'D)
Decision Flow Diagram Depicting the 6-Step Process
in the DOE Risk Assessment Guideline

STEP 1

DEFINE YOUR SYSTEM

STEP 1

GENERAL PURPOSE OF STEP 1: The purpose of Step 1 is to develop a general definition of your system. The definition is developed by looking at several key system features: composition, connections, size, cost(s), and back-ups. First, the current configuration of your system is established to ensure that you have fully identified all system components and connections. Use of a diagram provides a visual record of your current system configuration. It also allows you to visualize potential vulnerabilities that may exist as a result of your system's connections and data flows. Second, Step 1 helps you in developing a general cost estimate for your system so that you are able to appreciate how much it would cost to replace it in its entirety. It is also important to have a general appreciation for the cost of your system in order to decide which, if any, countermeasures are justified based on the cost of your system. Step 1 also reviews the type of software and data used by your system, with the objective of understanding how much labor went into the development of each and whether back-ups are available and necessary.

STEP 1 END-PRODUCTS: (1) A system configuration diagram which depicts your system's major components and connections, (2) a current listing of your system's major components, and (3) cost estimates for replacing your system's hardware, software and data.

NOTE: It is important to realize that a site may facilitate multiple ADP systems. Each system requires an individual risk assessment in order to accurately analyze the existing state of each system.

IT IS RECOMMENDED THAT YOU REVIEW STEP 1 IN ITS ENTIRETY BEFORE STARTING. IF YOU ALREADY HAVE INFORMATION THAT FULFILLS THE OBJECTIVES OF STEP 1, AND/OR PREFER TO DEVELOP IT USING AN ALTERNATE RISK ASSESSMENT METHOD, YOU MAY PROCEED TO THE EXECUTIVE SUMMARY AND COMPLETE THE BLOCK FOR STEP 1. BE SURE TO NOTE WHAT SOURCES AND/OR METHODS WERE USED TO DEVELOP THIS INFORMATION. ATTACH COPIES OF ANY SUPPORTING DOCUMENTATION TO ENSURE THAT THE INFORMATION ENTERED ON YOUR EXECUTIVE SUMMARY IS FULLY SUPPORTED.

GETTING STARTED

1. Make copies of all the Worksheets and the Executive Summary so that your originals may be preserved and reused for subsequent assessments: a full set of the Worksheets and the 5 page Executive Summary are located in Volume II, Worksheets and Executive Summary.
2. Open to your copy of the Executive Summary and the Step 1 Worksheets in Volume II and review them. (Step 1 Worksheets are located at the Step 1 Worksheet tab in Volume II.)
3. Resource Tables are located in this Chapter following the appropriate instructions. Spread them out before you and fully familiarize yourself with them.
4. Obtain any materials that already exist which may be helpful in completing Step 1 and which might also be used as supporting documentation for attachment to the Executive Summary. Helpful materials include:

- Basic system configuration diagram depicting system components and interfaces: Possible sources include your Computer Protection Plan, Computer Security Plan, accreditation or certification documentation, configuration management plans, system diagrams, and your organization's computer support group.

- Existing inventories: Possible sources include your Computer Protection Plan, Computer Security Plan, accreditation or certification documentation, and/or inputs developed for the ADP Long Range Plan or the Computer Security Long Range Plan.

- General cost information: Possible sources include computer catalogs and advertisements, procurement organizations, and vendor price lists. Your organization's computer support group can also provide general cost information if necessary.

5. Proceed with Step 1 instructions.

INSTRUCTIONS FOR
WORKSHEET W1.1, SYSTEM CONFIGURATION AND CONNECTIONS

GENERAL PURPOSE OF WORKSHEET W1.1: The general purpose of this worksheet is to provide a current understanding of your system's components, configuration and interfaces. By reviewing (and updating if necessary) the configuration of your system, you can visually identify all major components of your system, its current interfaces, and any external connections. This understanding is critical in developing an appreciation for the number and type of components that would have to be replaced should your system be damaged, destroyed, or stolen, as well as for identifying potential system (and network) vulnerabilities (useful for addressing Step 4 later on in this process).

1. Complete Block 1 of the worksheet with your system's name/identification, primary organization/user, primary system use, location, and the date(s) that the risk assessment is being conducted. You may wish to devise an abbreviated form for the information requested in Block 1 of the worksheet that you can use on subsequent worksheets since all worksheets ask for identifying information. (It is important that at least some shortened form of system identification appear on each worksheet since the worksheets provide important back-up documentation for the risk assessment.)

2. Determine what type of connections your system has, if any, and check the appropriate box in Block 2 of the worksheet. The following definitions should be used in describing the type and characteristics of your system's connections:

- Local Area Network (LAN): A LAN is typically confined to a single building or may span several buildings (such as with a university campus or a multi-building laboratory community). The typical LAN radius is approximately 6-8 kilometers.
- Wide Area Network (WAN): Networks that cover a larger geographic area than that described above for a LAN are considered a wide area network (WAN).
- Closed Network: network where all access to the network is from network components located in a controlled access area or access to the network from outside of the controlled access area is via encrypted links or a protected distribution system.
- Open Network: A network with the capability to communicate with devices outside of the network's controlled access area, where all network communications outside of controlled access areas are not encrypted or protected by a protected distribution system.

3. Attach a system configuration diagram to the worksheet in Block 3 if one is available. If a diagram does not exist, develop a simple one. The diagram should indicate all major system components, their interfaces, and all external connections. The system manager or your organization's computer support group can provide assistance in developing the diagram if you are unsure about connections or specific system components. In addition, prepare a short (1/2 - 1 page) written description of your site and what is being included as the scope of your risk assessment (i.e., which systems, basic site security program, etc.).

4. Enter the information developed for this worksheet in the Step 1 block of the Executive Summary, Sections 1a, 1b, and 1c.

5. Proceed to Worksheet W1.2, Hardware Inventory and Cost.

INSTRUCTIONS FOR
WORKSHEET W1.2, HARDWARE INVENTORY AND COST

GENERAL PURPOSE OF WORKSHEET W1.2: The general purpose of this worksheet is to define the size of your system and to provide a general cost estimate for your system's components. The cost estimate is important because it provides a way to determine how much it would cost to replace your system, and also provides a figure for use in selecting the most appropriate security countermeasures for your system based on its value (useful in Steps 3 and 5 later in the process).

1. Complete Block 1 of the worksheet identifying your system.
2. Review Resource Table R1.2A (Small/Simple System) and Resource Table R1.2B (Large/Complex System), Sections a and b, to define your system's size/type. Section a of each Resource Table provides a general definition of the two system size/types. Section b of each Resource Table provides a list of generic computer types and hardware components that are characteristic of the system size/type. Note that system components include the computer, printer, peripherals, environmental products, and special support items.
3. Turn to your Executive Summary and in Section 1d, mark the box for your system's size/type, and select which generic type of system you have.
4. Locate a recent inventory of your system and its components for attachment here. If an inventory does not exist, briefly list* the major hardware components of your system in Block 2, Hardware Inventory. Note that it is perfectly acceptable to group common components together when listing your system's components (e.g., 12 tape drives, 2 printers, etc.) Refer again to Resource Tables R1.2A and R1.2B, Section b, for a listing of generic computer types and hardware components for your consideration to ensure that all major components are noted. If cost information readily exists for the components of your system, you may list the actual dollar amounts for them. However, it is perfectly acceptable to review Section c of the Resource Table R1.2A or R1.2B, estimate the total cost for your system's components, and select a cost rating (VL - VH) for your system's hardware. Remember, the objective here is to develop an estimate of your system's cost -- NOT a down to the dollar figure on an item by item basis.
5. Complete Block 3 of Worksheet W1.2, Total Replacement Cost, by providing a total APPROXIMATE replacement cost figure for your system's hardware; -OR- Select a cost rating from the cost rating scheme (VL -VH) that best reflects the total cost of replacing your hardware. The primary (main) assets (vs. peripherals or other support equipment) should drive the overall rating chosen (e.g., CPU = H, printer = VH, auxiliary printer = VH; the overvall rating = H).
6. Go to Block 1e of the Executive Summary, Summary of System Replacement Costs, and mark the box of the cost rating (VL - VH) that most closely depicts the replacement cost for your hardware.
7. Proceed to Worksheet W1.3, Software Inventory and Cost.

*Note: Each inventory list in Step 1 is organized so that you may enter each major component individually in numeric order on the lines provided. If the length of your inventory exceeds the number of lines provided, you may make multiple copies of the Worksheet and continue your numbering on subsequent pages. Also, if you are assessing a group of systems, a copy of this worksheet can be used for each individual one.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

SMALL/SIMPLE SYSTEM:

- DEFINITION
- COMPONENTS
- COST GUIDANCE

STEP 1

**RESOURCE
TABLE
R1.2A**

a. DEFINITION OF A SMALL/SIMPLE SYSTEM:

A SMALL/SIMPLE COMPUTER DESIGNED PRIMARILY TO SUPPORT A SINGLE USER AT A TIME. DISK DRIVES, PRINTERS, AND OTHER EQUIPMENT ASSOCIATED WITH THE COMPUTER AND ITS USE ARE CONSIDERED PART OF THE SYSTEM.

b. TYPICAL COMPUTER TYPES AND COMPONENTS OF A SMALL/SIMPLE SYSTEM

<u>Computer Types</u>	<u>Hardware Components</u>	
<ul style="list-style-type: none"> • Memory Typewriter <ul style="list-style-type: none"> - Basic - Advanced • Word Processor <ul style="list-style-type: none"> - Basic - Advanced • Personal Computer <ul style="list-style-type: none"> - Basic - Advanced • CAD/CAM/Graphics Workstation <ul style="list-style-type: none"> - Basic - Intermediate - Advanced 	<ul style="list-style-type: none"> • Monitors • Storage Devices <ul style="list-style-type: none"> - Disk Drives - Tape Drives • Central Processing Unit • Peripherals <ul style="list-style-type: none"> - Switch Boxes - Plotters - Digitizers 	<ul style="list-style-type: none"> • Printers • Communications Support Equipment • Special Support Items <ul style="list-style-type: none"> - Surge Suppressors - Computer and Equipment Stands, Tables, etc. - Special Purpose Tables - Environmental Control Equipment

c. COST GUIDANCE FOR A SMALL/SIMPLE SYSTEM *

APPROXIMATE COST RANGE:	\$0 - \$5,000	\$5,001 - \$10,000	\$10,001 - \$25,000	\$25,001 - \$50,000	\$50,000+
COMPUTER TYPES:	<ul style="list-style-type: none"> • BASIC MEMORY TYPEWRITER • BASIC WORD PROCESSOR • BASIC PERSONAL COMPUTER 	<ul style="list-style-type: none"> • ADVANCED MEMORY TYPEWRITER • ADVANCED WORD PROCESSOR • ADVANCED PERSONAL COMPUTER • BASIC CAD/CAM/ GRAPHICS WORKSTATION 	<ul style="list-style-type: none"> • ADVANCED PERSONAL COMPUTER • INTERMEDIATE CAD/CAM/ GRAPHICS WORKSTATION - CPU SYSTEM 	<ul style="list-style-type: none"> • INTERMEDIATE-ADVANCED CAD/CAM/ GRAPHICS WORKSTATION - CPU SYSTEM 	<ul style="list-style-type: none"> • ADVANCED CAD/ CAM/GRAPHICS WORKSTATION - CPU SYSTEM - MINI-COMPUTER CAPABILITIES - PERIPHERAL DEVICES FOR MEMORY
-- PLUS ALL OTHER COMPONENTS OF THE SYSTEM --					
COST RATING:	VERY LOW (VL)	LOW (L)	MEDIUM (M)	HIGH (H)	VERY HIGH (VH)

* NOTE: A system's cost rating should reflect the sum of all system components: computer, printer, peripherals, and support items.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

LARGE/COMPLEX SYSTEM:

- DEFINITION
- COMPONENTS
- COST GUIDANCE

STEP 1

**RESOURCE
TABLE
R1.2B**

a. DEFINITION OF A LARGE/COMPLEX SYSTEM:

A COMPUTER SYSTEM WHICH USES ITS RESOURCES, INCLUDING I/O DEVICES, STORAGE, CENTRAL PROCESSORS, CONTROL UNITS, AND SOFTWARE PROCESSING CAPABILITIES TO ENABLE ONE OR MORE USERS TO MANIPULATE DATA AND PROCESS PROGRAMS IN AN APPARENTLY SIMULTANEOUS MANNER. SUCH SYSTEMS HAVE ONE OR MORE OF THE CAPABILITIES KNOWN AS TIME-SHARING, MULTI-PROGRAMMING, MULTI-ACCESSING, MULTI-PROCESSING, OR CONCURRENT PROCESSING.

b. TYPICAL COMPUTER TYPES AND COMPONENTS OF A LARGE/COMPLEX SYSTEM

<u>Computer Types</u>	<u>Hardware Components</u>	
<ul style="list-style-type: none"> • CAD/CAM/Graphics Workstation <ul style="list-style-type: none"> - Advanced • Mini-Computer • Mainframe Computer • Super-Computer 	<ul style="list-style-type: none"> • Terminals/Monitors <ul style="list-style-type: none"> - Smart - Dumb • Consoles • Storage Devices <ul style="list-style-type: none"> - Arrays - Disk Drives - Tape Drives - Cartridge Tape Drives - Storage Servers - Storage Controllers • Central Processing Unit • I/O Processors • Printers <ul style="list-style-type: none"> - Dot Matrix - Laser - Line Printer 	<ul style="list-style-type: none"> • Other Peripherals <ul style="list-style-type: none"> - Color Plotters - Digtizer - Table Plotters - Drum Plotters • Communications Equipment • Environmental Products <ul style="list-style-type: none"> - Power Conditioners - Power Distribution Systems - Transient Voltage Suppressors - Uninterrupted Power Systems - A/C and Other Environmental Control Equipment • Special Support Items <ul style="list-style-type: none"> - Special Stands and Tables - Partitions - Storage Cabinets - Tables, etc.

c. COST GUIDANCE FOR A LARGE/COMPLEX SYSTEM *

APPROXIMATE COST RANGE:	\$50,000 - \$250,000	\$250,001 - \$750,000	\$750,001 - \$2.5 M **	\$2.5 M - \$8.0 M	\$8.0 M+
COMPUTER TYPES:	<ul style="list-style-type: none"> • ADVANCED CAD/CAM/CASE WORKSTATION <ul style="list-style-type: none"> - CPU SYSTEM - PERIPHERAL STORAGE DEVICES - SINGLE PROCESSOR • MINI-COMPUTER 	<ul style="list-style-type: none"> • MINI-COMPUTER <ul style="list-style-type: none"> - PROCESSOR - INCREASED MEMORY STORAGE 	<ul style="list-style-type: none"> • MINI-COMPUTER • MAINFRAME COMPUTER <ul style="list-style-type: none"> - EXTENSIVE MASS-STORAGE CAPACITY 	<ul style="list-style-type: none"> • MAINFRAME COMPUTER <ul style="list-style-type: none"> - EXTENSIVE MASS-STORAGE CAPACITY - MULTIPLE COMMUNICATIONS LINE CAPACITY - REQUIRES CONTROLLED OPERATING ENVIRONMENT (COMPUTER ROOM) 	<ul style="list-style-type: none"> • LARGE MAINFRAME COMPUTER • SUPER-COMPUTER <ul style="list-style-type: none"> - SUPERIOR MASS-STORAGE CAPACITY - REQUIRE CONTROLLED OPERATING ENVIRONMENT (COMPUTER ROOM) - MULTIPLE COMMUNICATIONS LINE CAPACITY - STATE-OF-THE-ART PROCESSING CAPACITY
-- PLUS ALL OTHER COMPONENTS OF THE SYSTEM --					
COST RATING:	VERY LOW (VL)	LOW (L)	MEDIUM (M)	HIGH (H)	VERY HIGH (VH)

* NOTE: A system's cost rating should reflect the sum of all system components: computer, printer, peripherals, and support items.

** M = Million

INSTRUCTIONS FOR
WORKSHEET W1.3, SOFTWARE INVENTORY AND COST

GENERAL PURPOSE OF WORKSHEET W1.3: The general purpose of this worksheet is four-fold. First, it will help you develop an accurate and up-to-date appreciation of the various software (applications, programs) used on or by your system. Second, it will allow you to develop a rough estimate of the cost of replacing your software. This is important in determining which security measures may be merited for the protection of your software based on its value. Third, the worksheet focuses on whether back-ups exist for your system's software, and whether they should be instituted. Finally, the worksheet allows you to identify the type of storage media your software uses which will be of use in selecting the proper measures to protect it.

1. Complete Block 1 of Worksheet W1.3, identifying your system.
2. Review Sections a and b of Resource Table R1.3 to recall and list the various types of software your system uses. If you do not have a software inventory, list your software (applications, programs) in Block 2 (columns a and b) of the Software Inventory and Cost Worksheet.
3. Review Section c of Resource Table R1.3 to note the various types of storage media that your system may utilize. After reviewing this list, complete column 2 (c) (Type Storage Media) and 2 (d) (Does a Back-Up Exist?) on the Software Inventory and Cost Worksheet.
4. Review Sections d and e of Resource Table R1.3 to understand the cost guidance provided for use in estimating the cost of replacing your software. If your software is "off-the-shelf," approximate its cost and either enter the \$ amount in column (f) of the Worksheet (\$ Amount) AND/OR enter the appropriate cost rating (VL - VH) that reflects an approximate off-the-shelf cost for your software. To do this, use the guidance provided in Section d of the Resource Table. If the software is not commercially available, approximate the total amount of hours that would be required to replace (redevelop) the software. Enter this number in column (e) of the Worksheet (Approx. Hours to Develop). Then calculate the replacement cost using the guidance provided in section (e) of Resource Table R1.3 (Guidance for Calculating Software Replacement Costs). If you would prefer to use actual labor rates, you may consult the sources identified in this section of the worksheet. It should be noted that software replacement costs should only be calculated in cases where there is not a back-up copy stored in an off-site location. Therefore, labor costs to recreate lost data would only be for the period of development not yet protected by back-ups. Enter the \$ amount for replacing the software in the Worksheet column (f) (\$ Amount) AND/OR enter the appropriate cost rating (VL - VH) in column (g) (Rating). Again, remember, the objective here is NOT to develop down to the dollar replacement costs. Approximates are the goal.
5. Complete Block 3 of Worksheet W1.3 with the total replacement cost for all of your system's software with EITHER a \$ estimate or the appropriate cost rating (VL-VH).
6. Review your list of software groups, the status of their back-ups, and the cost rating you assigned for their replacement cost. Place a star (*) in the margin next to any entry that (a) does not have a back-up AND (b) was assigned a cost rating of Medium, High, or Very High. You now can readily identify any software for which back-ups should be immediately developed. Those with a Very High rating, should be considered for off-site storage.
7. Complete Block 1e on the Executive Summary indicating the cost rating chosen for replacing all of the software used by your system. Complete Block 1f on the Executive Summary indicating the status of back-ups for your system's software.
8. Proceed to Worksheet W1.4 Software Inventory and Cost.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT	. SOFTWARE: TYPES, USES, STORAGE MEDIA	STEP 1
	. SOFTWARE AND DATA COST GUIDANCE	RESOURCE TABLE R1.3

a. TYPES OF SOFTWARE TO CONSIDER FOR SOFTWARE INVENTORY:

- | | |
|--|---|
| <ul style="list-style-type: none"> • Off-the-Shelf Software <ul style="list-style-type: none"> - Word Processing - DBMS - Graphics • Applications Software | <ul style="list-style-type: none"> • Encryption Software • Operating Software • Security Related Software • Utilities Software • Communications Software |
|--|---|

b. SAMPLE SUBJECT AND FUNCTION AREAS FOR SOFTWARE AND DATA USE:

- | | |
|---|--|
| <ul style="list-style-type: none"> • Accounting/Financial • Administration • Contract Management/ Administration • Engineering/Scientific | <ul style="list-style-type: none"> • Personnel Management • Manufacturing/Control • Mathematics/Statistical • Security • Training |
|---|--|

c. SAMPLE TYPES OF STORAGE MEDIA:

- | | | |
|----------|---------------|--|
| a. TAPES | d. CARTRIDGES | g. MASS MEMORY STORAGE UNIT
(REMOVABLE/NON-REMOVABLE) |
| b. DISKS | e. CYLINDERS | |
| c. DRUMS | f. CARDS | h. HARD COPY OUTPUT |
| | | i. OPTICAL DISCS |

d. COST GUIDANCE FOR SOFTWARE AND DATA:

COST RATING	VERY LOW (VL)	LOW (L)	MEDIUM (M)	HIGH (H)	VERY HIGH (VH)
CURRENT PURCHASE PRICE OR DEVELOPMENT COST	\$0 - 5,000	\$5,001 - 10,000	\$10,001 - 25,000	\$25,001 - 50,000	\$50,000+

e. GUIDANCE FOR CALCULATING SOFTWARE AND DATA REPLACEMENT COSTS:

- For "Off-the-Shelf" Software Prices:
 - Consult computer catalogs and advertisements, as well as government price schedules and local vendor price lists available from your organization's computer support group or Procurement Office

- For Software and Data Development Costs:
 - Consult contract labor cost rates available from the Procurement Office or the contract's COTR

OR

 - Develop the total cost by multiplying approx. hours spent times average labor cost per hour. Accepted labor costs for your use are provided:
 - .. Clerical: \$5-10/hr.
 - .. Junior Professional or Programmer: \$15-20/hr.
 - .. Senior Professional or Programmer: \$20-30/hr.

- Approximate No. of work hours per: (Holidays and weekends are not included)
 - 1 Year: 2,080
 - 6 Months: 1,040
 - 1 Month: 170

INSTRUCTIONS FOR
WORKSHEET W1.4, DATA INVENTORY AND COST

GENERAL PURPOSE OF WORKSHEET W1.4: The purpose of this worksheet is to identify all data used by your system. It is important to understand which data your system utilizes for several reasons. It allows you to understand the overall value of these data in terms of approximately how many hours it took to develop it and would take to replace it. This worksheet also focuses on whether back-up data exist, and whether those that exist are sufficient.

1. Complete Block 1 of Worksheet W1.4, identifying your system.
2. Determine whether an inventory exists for the types or categories of data you use in conjunction with your system. If one exists, obtain it for use in completing columns (b) - (f) of the Worksheet. If no inventory or an incomplete inventory exists, list the major types or categories of data used by your system in column (a) of the Worksheet. Again, remember that it is perfectly acceptable to group data by categories (e.g., Salary-related, Equal Employment Opportunity-related, Medical Benefits, etc.) Assign a sequential number to each entry (D-1, D-2, and so on). Again, if additional room is required for the list, make additional copies of this worksheet.
3. Turn to column (c) on the Worksheet, and for each data category listed on the inventory, estimate approximately how many hours it would take to recreate it if it had to be replaced. In addition, note in column (d) whether back-up copies of these data exist.
4. To determine the replacement cost for these data, approximate the number of hours that would be required to recreate it and multiply this number by the labor cost figures provided in Section e of Resource Table R1.3. Again, precise down to the dollar amounts are not necessary; estimates are perfectly acceptable and use of the cost rating scheme (VL - VH) instead of replacement costs is encouraged.
5. Complete Block 3 of Worksheet W1.4 with the total cost, either a \$ estimate or a cost rating (VL to VH), for replacing the data used by your system.
6. Review your data inventory list (column b), the status of their back-up copies (column d), and the cost rating you assigned for their replacement cost (column f). Place a star (*) in the margin next to any entry that (1) did not have a back-up and (2) was assigned a cost rating of Medium, High, or Very High. You have now identified data for which back-up copies are strongly recommended.
7. Turn to the Executive Summary, Step 1, and complete Block 1f indicating the cost rating (VL-VH) that reflects the cost of replacing all data used by your system.
8. Complete Block 1f of the Executive Summary, Step 1, indicating the status of back-up copies for your data.
9. Proceed to Step 2, Characterize Your System, Software, and Data.

STEP 2

GENERAL PURPOSE OF STEP 2: The purpose of Step 2 is to characterize your total system in terms of several key characteristics. Step 2 worksheets ask questions in two primary areas:

1. Does your system process any classified information or sensitive unclassified information? If so, what types/levels? Responses to these questions provide the basis for selecting what type(s) of security precautions are required for your system, software and data.
2. How important is your system, its operations, software and data to its users and their organization? Responses to this question will help you to determine the relative importance of the system, software, and data, and provide the basis for determining or validating your contingency planning needs.

STEP 2 END-PRODUCTS: (1) An assessment of the relative importance of your system, software, and data to their users and organization; and (2) an identification of what types of information you are processing (e.g., unclassified, sensitive unclassified, or classified).

IT IS RECOMMENDED THAT YOU REVIEW STEP 2 IN ITS ENTIRETY BEFORE STARTING. IF YOU ALREADY HAVE INFORMATION THAT FULFILLS THE OBJECTIVES OF STEP 2, AND/OR PREFER TO DEVELOP IT USING AN ALTERNATE RISK ASSESSMENT METHOD, YOU MAY PROCEED TO THE EXECUTIVE SUMMARY AND COMPLETE THE BLOCK FOR STEP 2. BE SURE TO NOTE WHAT SOURCES AND/OR METHODS WERE USED TO DEVELOP THIS INFORMATION. ATTACH COPIES OF ANY SUPPORTING DOCUMENTATION TO ENSURE THAT THE INFORMATION ENTERED ON YOUR EXECUTIVE SUMMARY IS FULLY SUPPORTED.

GETTING STARTED

1. Open to your copy of the Executive Summary and the Step 2 Worksheets and review them. (Step 2 Worksheets are located at the Step 2 Worksheet tab in Volume II.)
2. Step 2 Resource Tables are located with the Step 2 instructions. It is recommended that you familiarize yourself with the information provided on them before starting Step 2.
3. Obtain any materials that already exist which may be helpful in completing Step 2 and which might also be used as supporting documentation for attachment to the Executive Summary. Useful existing materials include: results of prior efforts to identify the sensitivity or classification of the software (applications/programs) and data used on or by your system; and existing contingency plans which provide an analysis of why a particular system merits a contingency program/plan.
4. Please read the NOTE on the Step 2 Worksheets W2.2 (Software Characteristics and Importance) and W2.3 (Data Characteristics and Importance). These worksheets allow you to list the software and data that were inventoried in Step 1 by their reference number, thereby avoiding relisting all these entries.
5. Proceed with Step 2 instructions.

INSTRUCTIONS FOR
WORKSHEET W2.1, SYSTEM CHARACTERISTICS AND IMPORTANCE

GENERAL PURPOSE OF WORKSHEET W2.1: The general purpose of this worksheet is to determine the importance of your system. Importance here is measured in terms of: the number of users that utilize (and depend on) the system; the frequency with which the system is used; and the impact on you and your organization if the system were not available for use/operation. This simple review will allow you to readily identify the overall importance of your system to you and your organization, and whether the development and use of a contingency plan and procedures is advisable. If several systems have been grouped together for the purpose of this assessment, the Worksheet provides space for each system to be reviewed on an individual basis.

1. Review Resource Table R2.1 (Rating the Importance of A System, its Software and Data). Three separate "mini-tables" appear on this Resource Table: (a) Number of Users, (b) Frequency of Use, and (c) Impact if Unavailable. Be sure to read the explanations included with each mini-table to fully understand the rating schemes (VL - VH) provided for each mini-table.
2. **If several systems were addressed on this worksheet because a single risk assessment is being conducted on them as a group, and the ratings for each system differ, then separate recommendations should be developed regarding system contingency planning needs and additional security measures.**
3. Determine the appropriate rating for your system (Very Low to Very High) using Section a (Number of Users). Record your answer in column (b) of Worksheet W2.1. (Note that two rating schemes are provided: one for small/simple systems and one for large/complex systems. Select the rating appropriate for the size/type of system that you are assessing, based on your Step 1 results.)
4. Turn to Section (b) of the Resource Table (Frequency of Use) and determine the appropriate rating for your system (VL - VH) for your system. Enter the rating on your worksheet in column (c) Frequency of Use.
5. Turn to section (c) of the Resource Table (Impact if Unavailable) and determine the appropriate rating for your system (VL - VH). Enter the rating under column (d) of the worksheet.
6. If any of your ratings are Medium, High, or Very High, circle them. Ratings in the mid to high range point out a moderate to critical need for the development and use of a system contingency plan and procedures, and the implementation of more stringent security measures.
7. Summarize the results of this review in Step 2 of the Executive Summary, Block 2.b.1 (System) by checking the box with the ratings your selected (VL - VH) for each area of concern: Number of Users, Frequency of Use, and Impact if Unavailable.
8. Proceed to Worksheet W2.2, Software Characteristics and Importance.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT	RATING THE IMPORTANCE OF A SYSTEM, ITS SOFTWARE AND DATA				STEP 2
					RESOURCE TABLE R2.1

a. NUMBER OF USERS (SYSTEM AND CORRESPONDING RATING):					
Small/Simple System:	1	2	3-4	5	6+
Large/Complex System:	1-5	6-15	16-35	36-75	75+
Rating:	Very Low (VL)	Low (L)	Medium (M)	High (H)	Very High (VH)

b. FREQUENCY OF USE (SYSTEM, SOFTWARE AND DATA):					
Usage:	Periodic	Monthly	Weekly	Daily	Continuous
Rating:	Very Low (VL)	Low (L)	Medium (M)	High (H)	Very High (VH)

EXPLANATIONS:

- Periodic Usage = Occasional use during month
- Monthly Usage = Regular use during month
- Weekly Usage = Regular use during week
- Daily Usage = Regular use during day
- Continuous Usage = Continuous use during workday (8 hrs.) or use round-the-clock

c. IMPACT IF UNAVAILABLE (SYSTEM, SOFTWARE AND DATA):					
Importance to Organization or Operations:	Routine	Moderately Important	Important	Highly- Important	Vital
Rating:	Very Low (VL)	Low (L)	Medium (M)	High (H)	Very High (VH)

EXPLANATIONS:

- Routine = No impact on organization/capability
- Moderately Important = Month until impact on organization/capability
- Important = Week until impact on organization/capability
- Highly Important = Two days until impact on organization/capability
- Vital = Immediate impact on organization/capability

INSTRUCTIONS FOR
WORKSHEET W2.2, SOFTWARE CHARACTERISTICS AND IMPORTANCE

GENERAL PURPOSE OF WORKSHEET W2.2: The purpose of this worksheet is two-fold: First, it is used to determine whether your software (applications, programs) are involved in any sensitive unclassified or classified processing. This determination is accomplished through review of the categories provided on Step 2 Resource Tables R2.2a (Types and Examples of Sensitive Unclassified Data and Software) and R2.2b (Types of Classified Data and Software). Second, the worksheet determines the overall importance of your software (applications, programs) to its user(s) and their organization. Importance is defined in terms of: the frequency with which a given software (application, program) is used, and the impact on you (and your organization and its mission) if a given software (application, program) were unavailable. The impacts of unavailability might include a significant production delay, a missed payroll, or the inability to continue a high-cost experiment involving numerous other participants and high-cost equipment. Note: If a software package (application, program) retains data, then it must also be evaluated based upon the importance, value and classification of that data.

1. Complete Block 1 of the worksheet identifying your system.
2. Review Resource Tables R2.2a (Types and Examples of Sensitive Unclassified Software and Data) and R2.2b (Types of Classified Data and Software).
3. List the reference numbers of your software in column (2) of the worksheet. (You probably want to leave your copy of the Step 1 Worksheet W1.3 (Software Inventory and Costs) in plain view so that you can rapidly identify each item and its corresponding reference number.) Then, using Resource Tables R2.2a and R2.2b for guidance, review the software (applications, programs) used on your system. If your system is not involved in any classified or sensitive unclassified processing, place a mark in column (a.1 - unclassified). If your software (applications, programs) conducts sensitive unclassified processing, place a mark in column a.2 - sensitive unclassified; if applicable, check the box(es) indicating the type. If classified processing is involved, place a check in the final column (a.3 - classified) and indicate the highest classification level involved, and the mode of operation. In Block 3 of the worksheet, Approximate % Split, provide a rough estimate of the split between the 3 types of processing conducted (e.g., unclassified, sensitive unclassified, and classified). Use increments of 10 --10%, 20%, 30% up to 100%.
4. Now turn back to Resource Table R2.1 (Rating the Importance of A System, its Software, and Data). Using the rating schemes provided for Frequency of Use (Section b) and Impact if Unavailable (Section c), provide a rating (Very Low to Very High) for each of the Software entries on the Worksheet in column b (Frequency of Use) and column c (Impact if Unavailable).
5. If any of your ratings are Medium, High, or Very High, circle them. Such ratings provide additional rationale for the use of back-ups, the development of procedures for contingency situations, and the possible application of additional security measures.
6. Summarize the results of this review in Step 2 of the Executive Summary, Block 2a.1 and 2b.2.
7. Proceed to Worksheet W2.3, Data Characteristics and Importance.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**TYPES AND EXAMPLES OF
SENSITIVE UNCLASSIFIED
DATA AND SOFTWARE**

STEP 2

**RESOURCE
TABLE
R2.2a**

TYPE	EXPLANATION	EXAMPLE(S)
<p>a. VITAL RECORDS</p>	<ul style="list-style-type: none"> RECORDS ESSENTIAL FOR MAINTAINING CONTINUITY OF GOVERNMENT ACTIVITIES DURING A NATIONAL EMERGENCY 	<ul style="list-style-type: none"> EMERGENCY OPERATIONS RECORDS <ul style="list-style-type: none"> GENERAL MANAGEMENT RECORDS EMERGENCY MISSION RECORDS OTHER RIGHTS AND INTERESTS RECORDS <ul style="list-style-type: none"> LEGAL RIGHTS RECORDS FISCAL RECORDS OTHER
<p>b. PRIVACY ACT INFORMATION</p>	<ul style="list-style-type: none"> RECORDS MAINTAINED ON AN INDIVIDUAL THAT CONTAINS A NAME, IDENTIFYING NUMBER OR SYMBOL, OR PARTICULARS ASSIGNED TO AN INDIVIDUAL 	<ul style="list-style-type: none"> PAY AND RETIREMENT BENEFITS RECORDS MEDICAL AND PSYCHOLOGICAL RECORDS EDUCATIONAL ACHIEVEMENT RECORDS FINANCIAL TRANSACTIONS OTHER
<p>c. UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI)</p>	<ul style="list-style-type: none"> CERTAIN UNCLASSIFIED GOVERNMENT INFORMATION PROHIBITED FROM UNAUTHORIZED DISSEMINATION 	<ul style="list-style-type: none"> ATOMIC ENERGY DEFENSE PROGRAMS INFORMATION PRODUCTION OR UTILIZATION FACILITIES DESIGN SECURITY MEASURES ON SNM <ul style="list-style-type: none"> PRODUCTION OR UTILIZATION FACILITIES IN STORAGE IN TRANSIT FORMERLY RESTRICTED DATA ON <ul style="list-style-type: none"> DESIGN, MANUFACTURE, UTILIZATION OF NUCLEAR WEAPONS OR COMPONENTS OTHER
<p>d. OFFICIAL USE ONLY (OUO)*</p>	<ul style="list-style-type: none"> UNCLASSIFIED INFORMATION WHICH MAY BE EXEMPT FROM PUBLIC RELEASE UNDER THE FREEDOM OF INFORMATION ACT. 	<ul style="list-style-type: none"> DOE INTERNAL CORRESPONDENCE WORKING PAPERS ON DEFENSE PROGRAMS OTHER
<p>e. NATIONAL SECURITY RELATED (BUT UNCLASSIFIED)</p>	<ul style="list-style-type: none"> UNCLASSIFIED INFORMATION WHICH, ALONE OR IN THE AGGREGATE, REVEALS INFORMATION REGARDING A HIGH-VALUE U.S. PROGRAM OR INITIATIVE. UNCLASSIFIED INFORMATION DEVELOPED AND STORED REGARDING DOE MISSION(S) 	<ul style="list-style-type: none"> INTERNATIONAL TRAFFIC IN ARMS CONTROL UNCLASSIFIED INTELLIGENCE INFORMATION CONTROLLED SCIENTIFIC AND TECHNICAL INFORMATION <ul style="list-style-type: none"> NUCLEAR NON-PROLIFERATION ACT RELATED NAVAL NUCLEAR REACTOR PROGRAM RELATED STRATEGIC DEFENSE INITIATIVE RELATED MILITARY CRITICAL TECHNOLOGIES LIST FOREIGN EXCHANGE INFORMATION OTHER
<p>f. DOE SECURITY OR MISSION RELATED</p>	<ul style="list-style-type: none"> UNCLASSIFIED INFORMATION DEVELOPED AND STORED TO ADMINISTER AND ENSURE COMPLIANCE WITH DOE SECURITY PROGRAMS UNCLASSIFIED INFORMATION DEVELOPED AND STORED REGARDING DOE MISSION(S) 	<ul style="list-style-type: none"> LIFE ESSENTIAL MISSION ESSENTIAL IRRECOVERABLE INFORMATION LIMITED ACCESS INFORMATION SECURITY/INTERNAL AUDIT INFORMATION INVESTIGATION/LAW EXPERIMENT INFORMATION LEGAL INFORMATION AUDIT INFORMATION CONTRACT AND PROPRIETARY INFORMATION AUTOMATED DECISION-MAKING INFORMATION OTHER
<p>g. GOVERNMENT COMMERCIAL CONFIDENTIAL INFORMATION</p>	<ul style="list-style-type: none"> SENSITIVE COMMERCIAL INFORMATION NOT INCLUDING RESTRICTED DATA* GENERATED BY THE GOVERNMENT, THE RELEASE OF WHICH COULD PUT THE GOVERNMENT AT A COMPETITIVE DISADVANTAGE IN PROVIDING ENRICHMENT SERVICES 	<ul style="list-style-type: none"> PROGRAM-SPECIFIC INFORMATION R&D BREAKTHROUGHS OTHER
<p>h. INDIVIDUALLY IDENTIFIABLE ENERGY INFORMATION</p>	<ul style="list-style-type: none"> THIS IS AN EIA DESIGNATION AND REFERS TO COMPANY SPECIFIC INFORMATION THAT CAN BE READILY ATTRIBUTED TO THAT COMPANY 	<ul style="list-style-type: none"> OIL PRODUCTION AND COST DATA SPOT MARKET PRICES PAID

* POSSIBLE FUTURE CATEGORY

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT

• TYPES OF CLASSIFIED DATA
AND SOFTWARE

• MODES OF OPERATION

STEP 2

RESOURCE
TABLE
R2.2b

a. EXPLANATION OF MARKINGS

Classifications - Symbol	Categories - Symbol	Comments
Top Secret - TS Secret - S Confidential - C	Restricted Data - RD Formerly Restricted Data - FRD National Security Information - NSI	Both a classification and category are required on all DOE matter.

b. MARKINGS AND RELATIONSHIPS TO DOE CLEARANCES AND ACCESS AUTHORIZATION

Classification	Category	Access Authorization (Clearance)	DOE Badge Indicator
TS	RD	Q	1, 2
	FRD	Q, TS	1, 2, 3
	NSI	Q, TS	1, 2, 3
S	RD	Q	1, 2
	FRD	Q, TS, S, L	1, 2, 3, 4, 5
	NSI	Q, TS, S, L	1, 2, 3, 4, 5, 6
C	RD	Q, L	1, 2, 5
	FRD	Q, TS, S, L	1, 2, 3, 4, 5, 6
	NSI	Q, TS, S, L	1, 2, 3, 4, 5, 6

c. SPECIAL MARKINGS:

Information Marking	Explanation of Marking	Examples
PARD	Protect As Restricted Data	DOE Nuclear Weapons Program computations and material associated with a weapons code
CRYPTO	Cryptographic data	Classified or Unclassified information on cryptographic equipment, techniques or materials
WNINTEL	"Warning Notice - Intelligence Sources and Methods Involved."	Classified intelligence related data, sources, or methods
WD	Weapons data	Self-explanatory
Production Data	Weapon or material production data	Self-explanatory
CNWDI	Critical nuclear weapon design information	Self-Explanatory
COMSEC	Communications security	Telecommunications equipment, techniques or security information
NOFORN or NFD	No foreign dissemination	Information not to be released to foreign or third-country nationals
SRD, CRD SNSI, CNSI, etc.	Electronic transmissions abbreviations	Self-explanatory

d. MODES OF OPERATION:

MODE	EXPLANATION
SYSTEM HIGH SECURITY MODE	All system users in this environment must possess clearances and authorizations for all information contained in the system, and all system output must be clearly marked with the highest classification and all system caveats, until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and caveats have been affixed.
DEDICATED SECURITY MODE	The mode of operation in which the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.
MULTILEVEL SECURITY MODE	The mode of operation which allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present.
COMPARTMENTED SECURITY MODE	The mode of operation which allows the system to process two or more types of compartmented information or any one type of compartmented information with other than compartmented information. All system users need not be cleared for all types of compartmented information processed, but must be fully cleared for at least TOP SECRET information for unescorted access to the computer.

GENERAL PURPOSE OF WORKSHEET W2.3: The purpose of this worksheet is two-fold: First, it is used to determine whether the data used as input to or results from processing are sensitive unclassified or classified. This determination is accomplished through review of the categories provided on Step 2 Resource Tables R2.2a (Types and Examples of Sensitive Unclassified Data and Software) and R2.2b (Types of Classified Data and Software). Second, the worksheet determines the overall importance of these data sets to their user(s) and their organization. Importance is defined here in terms of: the frequency with which specific data sets are used, and the impact on you (and your organization and its mission) if certain data were unavailable. The impacts of unavailability might include a significant production delay, a missed payroll, or the inability to continue a high-cost experiment involving numerous other participants and high-cost equipment.

1. Complete Block 1 of the worksheet identifying your system.
2. Review Resource Tables R2.2a (Types and Examples of Sensitive Unclassified Software and Data) and R2.2b (Types of Classified Data and Software).
3. List the reference numbers of your data in column (2) of the worksheet. (You probably want to leave your copy of the Step 1 Worksheet W1.4 (Data Inventory and Costs) in plain view so that you can rapidly identify each item and its corresponding reference number.) Then, using Resource Tables R2.2a and R2.2b for guidance, review the data entries. If your system does not use any classified or sensitive unclassified data in processing, place a mark in column a.1 (unclassified). If your system uses sensitive unclassified data for processing, place a mark in column a.2 (sensitive unclassified); if applicable, check the box(es) indicating the type. If classified processing is involved, place a check in the final column a.3 (classified) and indicate the highest classification level of the data involved, and the mode of operation used by the system. In Block 3 of the worksheet, Approximate % Split, provide a rough estimate of the split between the 3 types of data processed by your system (e.g., unclassified, sensitive unclassified, and classified). Use increments of 10 --10%, 20%, 30% up to 100%.
4. Now turn to Resource Table R2.1 (Rating the Importance of A System, its Software, and Data). Using the rating schemes provided for Frequency of Use (Section b) and Impact if Unavailable (Section c), provide a rating (Very Low to Very High) for each of the Software entries on the Worksheet in column b (Frequency of Use) and column c (Impact if Unavailable).
5. If any of your ratings are Medium, High, or Very High, circle them. Such ratings provide additional rationale for the use of back-up copies, the development of procedures for contingency situations, and the possible application of additional security measures. Cross-check whether the entries meriting back-ups (e.g., those rated M, H, or VH) actually DO have back-ups. Refer to your answers regarding back-ups on the Step 1 Worksheets W1.3 and W1.4 to conduct this cross-check.
6. Summarize the results of this review in Step 2 of the Executive Summary, Block 2a.2 and 2b.3.
7. Proceed to Step 3, Review Baseline Security Requirements (BLSRs) and Identify Those Not Met or Partially Met.



STEP 3

REVIEW BASELINE SECURITY REQUIREMENTS (BLSRs)
AND IDENTIFY THOSE NOT MET OR PARTIALLY MET

STEP 3

GENERAL PURPOSE OF STEP 3: The purpose of Step 3 is to determine whether your system's hardware, software, and data -- as they exist today in their current operating environment and utilized by you and your organization -- meet the minimum Baseline Security Requirements (BLSRs) set forth in applicable DOE Orders. In the previous step you identified whether your system was involved in sensitive unclassified or classified processing. In this step, you are asked to review brief lists of security countermeasures (requirements) that **MUST** be in place, per DOE order, to protect such processing. For the majority of small/simple systems and stand alone large/complex systems (as defined in Step 1 of the Guideline) that are involved in sensitive unclassified processing, Step 3 will provide an adequate assessment of the current risks to your system. Therefore, upon completion of the BLSR, you will have conducted sufficient assessment of your risks to document the decisions made, accept or upgrade your current risk profile, and obtain management sign-off. During this step of the risk assessment, it may become obvious that the system's risk posture has been sufficiently assessed, evaluated, and accommodated. If it is found that all necessary BLSRs are satisfied you need only enter the appropriate information on the Executive Summary.

STEP 3 END-PRODUCTS: This Step will result in an assessment of your current security profile in terms of (1) whether you currently have met all of DOE's minimum baseline security requirements that apply to sensitive unclassified and classified ADP processing; (2) a list of any noted deficiencies; (3) a list of upgrades that are recommended to correct any noted deficiencies; and (4) target dates for correcting the noted deficiencies. Further, for the majority of small/simple systems (as defined in Step 1 of this process), the Step 3 results provide an adequate assessment of the current risks to your system. Therefore, Step 3 also documents the decisions made to accept or upgrade your current risk profile, and provides the basis for obtaining management sign-off for these decisions.

IT IS RECOMMENDED THAT YOU REVIEW STEP 3 IN ITS ENTIRETY BEFORE STARTING. IF YOU ALREADY HAVE INFORMATION THAT FULFILLS THE OBJECTIVES OF STEP 3, AND/OR PREFER TO DEVELOP IT USING AN ALTERNATE RISK ASSESSMENT METHOD, YOU MAY PROCEED TO THE EXECUTIVE SUMMARY AND COMPLETE THE BLOCK FOR STEP 3. BE SURE TO NOTE WHAT SOURCES AND/OR METHODS WERE USED TO DEVELOP THIS INFORMATION. ATTACH COPIES OF ANY SUPPORTING DOCUMENTATION TO ENSURE THAT THE INFORMATION ENTERED ON YOUR EXECUTIVE SUMMARY IS FULLY SUPPORTED.

GETTING STARTED

1. Open to your copy of the Executive Summary and the Step 3 worksheet. (The Step 3 Worksheets W3.1a - W3.8b, Review of Baseline Security Requirements are located at the Step 3 Worksheet tab in Volume II).
2. Turn to the Step 3 Resource Tables (located with the Step 3 directions) which provides the Master List of DOE Baseline Security Requirements (Resource Tables R3, pages 1 and 2). First note the titles of the Orders listed; these orders are all relevant to the security of DOE computer: facilities, personnel, documentation, systems, software, data, telecommunications, emissions, program administration and management, and operating environment. Note that column (a) in the left-hand column of the Master List contains an alphabetic code for each Order cited. These letter codes appear at the end of each requirement listed on Worksheets W3.1 - W3.8.

Turn to W3.1 for example and note that each entry is followed by a parentheses () containing a CAPITAL or lower-case letter. This letter designates the DOE document in which the particular requirement was stated so that if you need further clarification of a requirement, you may locate the appropriate Order.

The CAPITAL letter code is used for orders published by the unclassified computer security program and/or pertaining to the protection of sensitive unclassified information. The lower-case letter code is used for orders promulgated by the classified computer security program and/or pertaining to the protection of classified information. It should be noted, however, that there are a number of exceptions where a document applies to BOTH programs. These documents are marked with an (*). The Worksheets are also organized to reflect this: BLSRs are listed under one of the following categories: "Sensitive Unclassified;" "Classified;" or "Both."

3. Now look at the series of 8 Worksheets, each of which lists the minimum Base line Security Requirements (BLSRs) for a specific security discipline area. The 8 security discipline areas covered in this Step, along with the assets with which they are concerned, are listed below. As you review each discipline area, keep in mind your system (hardware, software, data); personnel; hard-copy information; operating environment; physical facility; communications interfaces; etc. Any stated applicable requirement that you cannot answer in the affirmative is a deficiency.

-Worksheet W3.1a and W3.1b, Review of BLSRs for Physical Security: This table sets forth minimum requirements for controlling access to and protecting the physical building, computing area/room, computing resources, support items, storage areas, and all human resources.

-Worksheet W3.2, Review of BLSRs for Personnel Security: This table sets forth minimum requirements for ensuring that personnel access to and use of computing resources (hardware, software, data) is properly controlled.

-Worksheet W3.3, Review of BLSRs for Information Security: This table sets forth minimum requirements for the protection of all hard-copy (non-electronic) information.

-Worksheet W3.4, Review of BLSRs for Communications: This table sets forth minimum requirements for the protection of all communications equipment, interfaces (wires, cables, lines, etc.), and the data transmitted on/by them in support of ADP processing/operations.

-Worksheet W3.5, Review of BLSRs for Emissions Security (TEMPEST): This table sets forth minimum requirements for the protection (from interception) of any emissions (signals, data) produced by electronic (ADP) systems.

-Worksheet W3.6a and W3.6b, Review of BLSRs for Computer Security: This table sets forth minimum requirements for the protection of the total ADP system (hardware, software, and electronically stored/processed data).

-Worksheet W3.7, Review of BLSRs for an organization's Administrative/ Procedural Security or Security Management: This table sets forth minimum requirements for the establishment and management of a security organization and program necessary to support day-to-day operations while meeting security procedural requirements. (It should be noted that procedures specific to a security discipline area, such as procedures for configuration management or system testing, are set forth under the appropriate security discipline (e.g., computer security in this example).

-Worksheet W3.8a and W3.8b, Review of BLSRs for Environmental Security and Safety: This table sets forth minimum requirements for ensuring that all ADP resources and personnel are protected from all environmental accidents, incidents, malfunctions, etc.

By reviewing the Baseline Security Requirements (BLSRs) in each category, you will be able to identify whether you have fully or partially met them, and whether major deficiencies exist in your security program.

4. Finally, obtain any materials that already exist which may be helpful in completing this BLSR review and/or which you may desire to use as supporting documentation for attachment to the Executive Summary. Helpful materials include results from prior: Compliance Reviews, audit results, security test and evaluation results, reports documenting the results of formal inspections and evaluations, internal site/facility/system procedural documentation, Computer Security Program Reviews, and Management Reviews. These materials should contain selected data regarding those areas where your system did not meet stated DOE requirements, along with recommendations regarding how the noted deficiencies were (to be) corrected. Should any of these materials partially or fully meet the objectives of Step 3, document this on the Executive Summary and reference or append this documentation.

5. Proceed to Step 3, Worksheets W3.1a - W3.1b, Baseline Security Requirements Review.

NOTE: It should be noted that the BLSRs set forth in these Resource Tables have been carefully cross-checked with the areas of inquiry set forth in the Safeguards and Security Standards and Criteria (Document "a") to ensure all standards and criteria are addressed in the Baseline Security Requirements provided here.

GENERAL PURPOSE OF WORKSHEETS W3.1 - W3.8: The general purpose of this series of worksheets is to provide a way to easily identify whether your system has fully met the requirements established for it (its operating environment and its users) as specified in all applicable DOE Orders. By reviewing the Baseline Security Requirements (BLSRs) in each category, you will be able to identify whether you have fully met the BLSRs, partially met them, whether major deficiencies exist, or whether it is not applicable. This worksheet also directs you to a list of countermeasures for your review from which you may select appropriate countermeasures to eliminate any noted deficiencies.

1. Begin your review of the BLSRs provided in the Worksheets. Use the following key to indicate in the box next to each stated requirement whether you have: Met the requirement (Y), Not Met The Requirement (NO), Only Partially fulfilled, or have met on paper but Do Not practice/use routinely (P). If a BLSR is not applicable, place N/A in the box. If you are unsure about a specific BLSR and its applicability to your system, refer back to the Master List in Resource Table R3 to identify from which Order the requirement was extracted. If you are still unsure, you may wish to consult the specific order cited. You may also wish to review the lists of BLSRs with appropriate representatives from physical security, personnel security, technical security, document control, and Health and Safety.

2. As you complete your review of the requirements stated for each security discipline area, record the results on the Executive Summary in the Step 3 Block under column (1a) (All Requirements Met) (Yes or No) or under column (1b) (Noted Deficiencies). If any deficiencies were identified, state in column (1c) (Will Do By) the date (month/year) by which the noted deficiency will be corrected. An identified deficiency is corrected by implementing the specific BLSR that has not, to date, been met. If your particular site/system is exempted from meeting a given BLSR, cannot comply with a specific BLSR, or a BLSR is not applicable to your system, so note this on Step 3 of the Executive Summary under column (d) (Comments and/or Supplemental Upgrades).

3. If no deficiencies were found in a given discipline area, you have met all the stated requirements. Turn to Block 2 at the bottom of the Executive Summary, Step 3. This Block asks you whether the results that you developed in Steps 1 and 2 regarding the overall value and importance of your hardware, software and data are significant enough to warrant upgrades of these security measures that already exist and fulfill the BLSRs.

4. If no supplemental countermeasures are merited, you may conclude the assessment here (unless your system, as defined in Steps 1 and 2, dictates use of Steps 4 and 5).

5. If, in your review, you met all the BLSRs but have decided that you would like to implement supplemental countermeasures in certain areas due to your Step 1 and 2 results, you should now consult the Resource Tables provided in Step 5. These tables (Countermeasures Guidance, Resource Tables R5.1a - R5.1h) provide lists of countermeasures also organized by security discipline area. Locate the discipline area(s) where you desire upgrades and review the countermeasures listed there. Note selected entries have a check mark next to them in the left hand margin. These check marks indicate that the particular countermeasure is generally easy to

implement at a fairly low cost. Select the countermeasure(s) necessary to supplement your existing program. Note any selection(s) in column (d), Comments and/or supplemental upgrades and enter the date you intend to complete the upgrade(s) in column (c), Will Do By.

6. If use of Steps 4 and 5 is not necessary, proceed to Step 6 and obtain the necessary sign-off from management indicating acceptance of your system's risk profile. If further assessment is necessary or desired based on the overall value and importance of your system, software and data, proceed to Step 4.

Finally, the worksheet allows you to end the risk assessment after completion of Step 3 if appropriate. You are asked to decide whether the value and importance of your system's hardware, software (applications, programs) and data support further, more detailed assessment. For the majority of small/simple systems (as defined in Step 1 of the Guideline), continuation will not be necessary.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**MASTER LIST OF
DOE SECURITY
REQUIREMENTS**

STEP 3

RESOURCE
TABLE
R3
(Page 1)

(a) BASELINE REQUIREMENT CODE *	(b) DOE DOCUMENT TITLE (As of September 1989)	(c) DOE DOCUMENT NUMBER **
A.	ESSENTIAL AND VITAL RECORDS PROTECTION PROGRAM	DOE 5500.7A
B.	PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI)	DOE 5635.4
(*) C.	MANAGEMENT OF AUTOMATED INFORMATION SYSTEMS AND DATA RESOURCES	DOE 1330.1B
(*) D.	ACQUISITION AND MANAGEMENT OF COMPUTING RESOURCES	DOE 1360.1A
E.	UNCLASSIFIED COMPUTER SECURITY PROGRAM	DOE 1360.2A
F.	SCIENTIFIC AND TECHNICAL INFORMATION PROGRAM	DOE 1430.2A
G.	POLICY FOR THE DISSEMINATION OF AND ACCESS TO DEPARTMENTAL UNCLASSIFIED SCIENTIFIC AND TECHNICAL INFORMATION	DOE 1430.3
H.	PRIVACY ACT	DOE 1800.1A
I.	MANAGING SCIENTIFIC AND TECHNICAL INFORMATION	DOE 1430.1A
J.	SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE	DOE 1360.4A
K.	INTERNAL CONTROL SYSTEMS	DOE 1000.3B
L.	USE OF TERMINALS AND MICROCOMPUTERS/WORD PROCESSORS OFF-SITE AS WELL AS PRIVATELY-OWNED ON- OR OFF-SITE	DOE 1360.7
a.	SAFEGUARDS AND SECURITY STANDARDS AND CRITERIA	N/A
(*) b.	TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST)	DOE 5300.2B
(*) c.	TELECOMMUNICATIONS: COMMUNICATIONS SECURITY	DOE 5300.3B
(*) d.	TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEM	DOE 5300.4B
(*) e.	FIRE PROTECTION	DOE 5480.7
(*) f.	STANDARD FOR FIRE PROTECTION OF DOE ELECTRONIC COMPUTER/DATA PROCESSING SYSTEMS	DOE/EP-0108

* NOTE: The code uses capital letters to specify Orders pertaining to the Unclassified Computer Security Program. Small case letters refer to Orders developed for the Classified Computer Security Program. However, it should be noted that selected Orders apply to both programs and are marked with an (*).

** NOTE: See Cross Reference List for numerical listing of Orders.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**MASTER LIST OF
DOE SECURITY
REQUIREMENTS**

STEP 3
RESOURCE
TABLE
R3
(Page 2)

(a) BASELINE REQUIREMENT CODE*	(b) DOE DOCUMENT TITLE (As of September 1989)	(c) DOE DOCUMENT NUMBER**
(*) g.	PERSONNEL SECURITY PROGRAM	DOE 5631.2B
h.	SAFEGUARDING OF NAVAL NUCLEAR PROPULSION INFORMATION	DOE 5630.8
(*) i.	VIOLATION OF LAWS, LOSSES, INCIDENTS OF SECURITY CONCERN	DOE 5631.5
(*) j.	PROTECTION PROGRAM OPERATIONS	DOE 5632.1A
k.	OPERATIONS SECURITY	DOE 5632.3B
(*) l.	PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIAL AND VITAL EQUIPMENT	DOE 5632.2A
m.	SECURITY SURVEYS, NUCLEAR MATERIALS SURVEYS AND FACILITY APPROVALS	DOE 5634.1A
n.	CONTROL OF CLASSIFIED DOCUMENTS AND INFORMATION	DOE 5635.1A
o.	TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM	DOE 5636.3A
p.	CLASSIFIED COMPUTER SECURITY PROGRAM	DOE 5637.1
q.	PHYSICAL PROTECTION OF CLASSIFIED MATTER	DOE 5632.5
(*) r.	PHYSICAL PROTECTION OF DOE PROPERTY AND UNCLASSIFIED FACILITIES	DOE 5632.6
(*) s.	PROTECTIVE FORCES	DOE 5632.7
(*) t.	PROTECTION PROGRAM OPERATIONS: SYSTEM PERFORMANCE TESTS	DOE 5632.8
(*) u.	ISSUANCE, CONTROL, AND USE OF BADGES, PASSES AND CREDENTIALS	DOE 5632.9
v.	CONTROL OF WEAPON DATA	DOE 5610.2
w.	MASTER SAFEGUARDS AND SECURITY AGREEMENTS	DOE 5630.13
x.	MANAGEMENT AND CONTROL OF FOREIGN INTELLIGENCE	DOE 5670.1

* NOTE: The code uses capital letters to specify Orders pertaining to the Unclassified Computer Security Program. Small case letters refer to Orders developed for the Classified Program. However, it should be noted that selected Orders apply to both programs and are marked with an (*).

** NOTE: See Cross Reference List for numerical listing of Orders.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**CROSS REFERENCE NUMERIC
LISTING OF DOE ORDERS USED TO
DEVELOP SECURITY
REQUIREMENTS**

STEP 3

**RESOURCE
TABLE R3
(Page 3)**

DOE DOCUMENT NUMBER	DOE DOCUMENT TITLE (As of September 1989)	BASELINE REQUIREMENT CODE
1000.3B	INTERNAL CONTROL SYSTEMS	K.
1330.1B	MANAGEMENT OF AUTOMATED INFORMATION SYSTEMS AND DATA RESOURCES	C.
1360.1A	ACQUISITION AND MANAGEMENT OF COMPUTING RESOURCES	D.
1360.2A	UNCLASSIFIED COMPUTER SECURITY PROGRAM	E.
1360.4A	SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE	J.
1360.7	USE OF TERMINALS AND MICROCOMPUTERS/WORD PROCESSORS OFF-SITE AS WELL AS PRIVATELY-OWNED ON- OR OFF-SITE	L.
1430.1A	MANAGING SCIENTIFIC AND TECHNICAL INFORMATION	I.
1430.2A	SCIENTIFIC AND TECHNICAL INFORMATION PROGRAM	F.
1430.3	POLICY FOR THE DISSEMINATION OF AND ACCESS TO DEPARTMENTAL UNCLASSIFIED SCIENTIFIC AND TECHNICAL INFORMATION	G.
1800.1A	PRIVACY ACT	H.
5300.2B	TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST)	b.
5300.3B	TELECOMMUNICATIONS: COMMUNICATIONS SECURITY	c.
5300.4B	TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEM	d.
5480.7	FIRE PROTECTION	e.
5500.7A	ESSENTIAL AND VITAL RECORDS PROTECTION PROGRAM	A.
5610.2	CONTROL OF WEAPON DATA	v.
5630.8	SAFEGUARDING OF NAVAL NUCLEAR PROPULSION INFORMATION	h.
5630.13	MASTER SAFEGUARDS AND SECURITY AGREEMENTS	w.
* 5631.1A	SECURITY EDUCATION PROGRAM	
5631.2B	PERSONNEL SECURITY PROGRAM	g.
5631.5	VIOLATION OF LAWS, LOSSES, INCIDENTS OF SECURITY CONCERN	i.
5632.1A	PROTECTION PROGRAM OPERATIONS	j.
5632.2A	PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIAL AND VITAL EQUIPMENT	l.
5632.3B	OPERATIONS SECURITY	k.
5632.5	PHYSICAL PROTECTION OF CLASSIFIED MATTER	q.
5632.6	PHYSICAL PROTECTION OF DOE PROPERTY AND UNCLASSIFIED FACILITIES	r.
5632.7	PROTECTIVE FORCES	s.
5632.8	PROTECTION PROGRAM OPERATIONS: SYSTEM PERFORMANCE TESTS	t.
5632.9	ISSUANCE, CONTROL, AND USE OF BADGES, PASSES AND CREDENTIALS	u.
5634.1A	SECURITY SURVEYS, NUCLEAR MATERIALS SURVEYS AND FACILITY APPROVALS	m.
5635.1A	CONTROL OF CLASSIFIED DOCUMENTS AND INFORMATION	n.
5635.4	PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI)	B.
5636.3A	TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM	o.
5637.1	CLASSIFIED COMPUTER SECURITY PROGRAM	p.
5670.1	MANAGEMENT AND CONTROL OF FOREIGN INTELLIGENCE	x.
DOE-EP-0108	STANDARD FOR FIRE PROTECTION OF DOE ELECTRONIC COMPUTER/DATA PROCESSING SYSTEMS	f.
N/A	SAFEGUARDS AND SECURITY STANDARDS AND CRITERIA	a.

* NOT ON MASTERLIST



STEP 4



REVIEW THREATS AND VULNERABILITIES AND
IDENTIFY ANY WHICH AFFECT YOUR SYSTEM

STEP 4

GENERAL PURPOSE OF STEP 4: The purpose of Step 4 is to conduct a review of the threats that might affect your system because of existing weaknesses or vulnerabilities in your system that could be exploited and cause a threat occurrence.

The Step 4 worksheet is organized to allow for the identification of threats to specific assets of your system and operating environment. It is completed using the Step 4 Resource Tables, (R4.1 - R4.7), which are organized as follows.

Four major threat categories are presented on each of the Step 4 Resource Tables:

- . Natural Threats
- . Intentional Human Threats (both insider and outsider)
- . Unintentional Human Threats (both insider and outsider)
- . Environmental Threats.

A resource table has been developed for each of the primary assets of the system and its operating environment. These assets include the:

- . Physical facility (building, computer room, supporting utilities, non-ADP equipment, supplies, etc.)
- . Personnel (computer operator(s), system manager, computer security official, data base administrator, etc.)
- . Information (hard-copy and electronically stored data, and electronic emissions)
- . Communications (lines, networks, COMSEC security devices, protected distribution systems, phones, modems, etc.)
- . Computer Hardware (CPU, peripherals, controllers, etc.)
- . Computer Software (operating system software, utilities software, applications software, etc.)
- . Procedures/Administration/Management (all procedural, administrative, and organizational functions, documentation, and general business practices that are necessary to effectively operate and use the system.)

Resource Table R4.1-4.6, Sample Impact of Threats to and Vulnerabilities of the Physical Facility, presents specific, real-world examples of these threats as they may affect the given asset. This two page set will help you think through various threat situations, combinations, and scenarios in order to postulate your specific threat situation(s).

As you review the Resource Tables in Step 4, also keep in mind the definitions for the four key impact areas: damage, destruction, disclosure, and denial.

- . Damage: This state exists when any asset, unintentionally or intentionally, suffers damage as a consequence of the threat, making the asset unusable until repairs/fixes can be made. Damage includes alteration and modification to data.
- . Destruction: This state exists when any asset, unintentionally or intentionally, is declared irreparable and irrecoverable due to threat induced destruction.
- . Disclosure: This state exists when unauthorized access to an asset occurs, causing information or data to be accessed by or released to someone without a clearance or a need to know. This includes the misuse of any data by someone with authorized access.
- . Denial (of Service): This state exists when computer services cannot be performed or made available within an acceptable period of time.

Keep in mind as you review the resource tables that these are only examples of the different threats and how they might impact a specific asset. To use the resource tables, think through whether or not a particular threat could occur because of existing system vulnerabilities. If the answer is yes, ask yourself what the impact might be if the threat occurred - damage of the asset, destruction of the asset, denial of use of the asset or unauthorized disclosure of information.

STEP 4 END-PRODUCTS: This Step will result in (1) a threat and vulnerability analysis of your system, facility, and its assets within its operating environment. It will also (2) allow you to identify which of the applicable threats are: very likely to occur, likely to occur, or unlikely to occur. Finally, Step 4 will provide the basis for determining which vulnerabilities should be corrected, and in what order, based on the simple probabilities identified for threat occurrence.

IT IS RECOMMENDED THAT YOU REVIEW STEP 4 IN ITS ENTIRETY BEFORE STARTING. IF YOU ALREADY HAVE INFORMATION THAT FULFILLS THE OBJECTIVES OF STEP 4, AND/OR PREFER TO DEVELOP IT USING AN ALTERNATE RISK ASSESSMENT METHOD, YOU MAY PROCEED TO THE EXECUTIVE SUMMARY AND COMPLETE THE BLOCK FOR STEP 4. BE SURE TO NOTE WHAT SOURCES AND/OR METHODS WERE USED TO DEVELOP THIS INFORMATION. ATTACH COPIES OF ANY SUPPORTING DOCUMENTATION TO ENSURE THAT THE INFORMATION ENTERED ON YOUR EXECUTIVE SUMMARY IS FULLY SUPPORTED.

GETTING STARTED

1. Open to your copies of the Executive Summary and the Step 4 Worksheet in Volume II. (Step 4 Resource Tables are included with Step 4 instructions.)

2. Familiarize yourself with the Step 4 Resource Tables. The Worksheets provide an overview of threat impacts. The Resource Tables provide specific real-world illustrations of how a particular threat could affect an asset in terms of destruction, damage, disclosure and denial of service. Also note that environmental threats are treated a little differently. Resource Table R4.7d is an acetate entitled "Map of DOE Facilities in the U.S" (located at the very back of Step 4). A key is also included that provides full facility titles for use in clarifying the acronym's used on the map. The acetate is for your use as an overlay when reviewing Resource Tables R4.7a - R4.7c that deal with the environmental threats of earthquakes, tornadoes, and thunderstorms in the continental United States.

3. Obtain any materials that already exist which may be helpful in completing Step 4 and/or which you may desire to use as supporting documentation for attachment to the Executive Summary. Helpful materials include your most recent Statement of Threat (where applicable), recent incident reports and historical records of security incidents for the last 5-10 years, any regionalized threat information developed to support threat and vulnerability assessments in your locality, and current/past Security Test Plans and results. If the existing materials meet the objectives of Step 4, document this in Step 4 of the Executive Summary, and reference or append this documentation.

If regionalized threat materials are not current or available, it is often worthwhile to contact your organization's security office for help in obtaining current crime statistics. Also note that the Annotated Bibliography, located on a floppy diskette which is included with this Guideline, provides a listing of current articles on threats and vulnerabilities for your use if you desire supplemental materials.

4. Proceed to Worksheet W4.1, Threats and Vulnerabilities of the Physical Facility.

GE

wh

an

no

in

no

tl

t

t

w

a

n

.

INSTRUCTIONS FOR
WORKSHEET W4.1-W4.6, THREAT AND VULNERABILITY REVIEW

GENERAL PURPOSE OF WORKSHEET W4.1-W4.6: The purpose of these Worksheets is to record which specific threats could impact your system, software, data, and operating environment due to existing deficiencies in your security profile. Further, these Worksheets also address the probability that a given threat could arise at your site or in your locality. (An uncomplicated probability scheme is provided for your use in the Note at the bottom of the Worksheet.) Step 4 of Executive Summary allows you to specify the priority in which the identified threat(s) should be treated.

1. Review the Step 4 Resource Tables (R4.1 - R4.7) and Worksheets (W4.1-W4.6) and think through how each specific threat could impact your assets. Using the Worksheets W4.1-W4.6, place a star next to any of the threats of concern; then circle the appropriate check mark(s) to indicate which impacts are the most worrisome. For your review of Resource Tables R4.7 (Environmental Threats), remove the acetate overlay from the binder and place it on top of each incident map to determine whether your locality is in a high risk area. Note any threats of concern and annotate all the other Resource Tables (under "Natural Threats") based on how the environmental threats impact your assets.

2. Summarize the threat impacts of greatest concern by asset area on Executive Summary Part 4, column (a). Provide a brief explanation, if needed, to clarify why and how a particular threat could impact your system.

3. Using the probability key provided here and at the bottom of Executive Summary Part 4, enter a High (H), Medium (M), or Low (L) probability rating in column (b) for the threat impacts you have listed on the Worksheet. These ratings will help you decide which threats and their impacts should be addressed as serious concerns, and in what specific order upgrades should be implemented.

Probability Key:

High (H)	= Threat is very likely to occur (more than once within a year).
Medium (M)	= Threat is likely to occur (only once every 5 years).
Low (L)	= Threat is unlikely to occur (only once every 10 years or less frequently).

4. Based on the probability ratings you provided, prioritize the order in which the upgrades that you recommend for dealing with these threat impacts should be implemented. You may sequentially rank the order in which these threats should be addressed (e.g., 1st, 2nd, 3rd, etc.) or you may wish to use the following scheme:

- (1) = Fix immediately
- (2) = Fix within the next 6-12 months
- (3) = Fix if and when resources are available.

5. After you have completed your review of all Step 4 Resource Tables and have entered the results on the Step 4 Executive Summary, it is suggested that you convene a meeting of colleagues who are knowledgeable about the system being assessed and who are conversant with security matters. Suggested team members include representatives from physical security, personnel security, technical security, document control, and Health and Safety. This informal meeting is suggested as a "sanity checkpoint" to discuss the results of your review in order to ensure completeness and provide different perspectives on possible threat scenarios and probabilities.

6. Proceed to Step 5, Countermeasures Review and Identification.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT	SAMPLE IMPACTS OF THREATS TO AND VULNERABILITIES OF THE PHYSICAL FACILITY	STEP 4
		RESOURCE TABLE R4.1
a. IMPACTS FROM NATURAL THREATS:		
<ul style="list-style-type: none"> • Building is destroyed by fire. • Computer facility is flooded by heavy rain and flood waters. • Computer facility is inaccessible because of sustained damages. • Sensitive information is disclosed to emergency personnel involved in facility evaluation during emergency. 		
b. IMPACTS FROM INTENTIONAL HUMAN THREATS :		
<ul style="list-style-type: none"> • Computer facility is destroyed by terrorist bombing. • Use of computer facility denied because of civil disorder outside facility. • Sensitive information disclosed because of unauthorized access to computer facility • Computer supplies damaged by vandals. 		
c. IMPACTS FROM UNINTENTIONAL HUMAN THREATS:		
<ul style="list-style-type: none"> • Sensitive information disclosed when computer operator forgets to lock the computer facility at end of the day. • Computer supplies destroyed when employee stores them in a damp area. • Computer facility damaged when maintenance personnel accidentally set off Halon fire suppression system. • Building becomes inaccessible when a toxic gas is released. 		
d. IMPACTS FROM ENVIRONMENTAL THREATS:		
<ul style="list-style-type: none"> • Computer facility becomes inaccessible because of failed heating system. • Building is destroyed after being condemned for structural failures. • Sensitive information is disclosed and computer facility damaged when support column for computer facility wall collapses. 		

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SAMPLE IMPACTS OF
THREATS TO AND
VULNERABILITIES OF
PERSONNEL**

STEP 4

**RESOURCE
TABLE
R4.2**

a. IMPACTS FROM NATURAL THREATS:

- Personnel are killed during an earthquake.
- Personnel are injured in a fire.
- Computer operators are unavailable because of injuries sustained during a tornado.

b. IMPACTS FROM INTENTIONAL HUMAN THREATS :

- Key personnel are taken hostage by terrorists.
- Key personnel are injured when assaulted by striking workers.
- Personnel are murdered when a bomb explodes.
- Sensitive information is disclosed by personnel when they are kidnapped and threatened.

c. IMPACTS FROM UNINTENTIONAL HUMAN THREATS:

- Computer operator is injured when moving some computer supplies.
- Systems manager dies after suffering heart attack.
- Data processing manager inadvertently discloses sensitive information to unauthorized individuals during meeting.

d. IMPACTS FROM ENVIRONMENTAL THREATS:

- Employee suffers heat exhaustion because of failed cooling system.
- Ceiling collapse causes the death of an employee.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SAMPLE IMPACTS OF
THREATS TO AND
VULNERABILITIES OF
INFORMATION, DATA,
AND EMISSIONS**

STEP 4

**RESOURCE
TABLE
R4.3**

a. IMPACTS FROM NATURAL THREATS:

- Data use denied because facility is inaccessible due to power failure.
- Data is destroyed by fire.
- Data base integrity damaged by effects of lightning.
- Sensitive data disclosed because tornado scatters storage media and hardcopy outputs throughout uncontrolled access area.

b. IMPACTS FROM INTENTIONAL HUMAN THREATS:

- Data base is destroyed through sabotage by authorized user who enters incorrect or false data.
- Data base damaged by a virus that alters selected files.
- Data base use denied because of theft by vandals.
- Classified or sensitive data disclosed through the interception of emissions.

c. IMPACTS FROM UNINTENTIONAL HUMAN THREATS:

- Data damaged by exposure to an electro-magnetic field.
- Data base destroyed by emotionally distraught employee.
- Data base unavailable because of errors in the DBMS software.
- Sensitive data disclosed because operator incorrectly patched output device.

d. IMPACTS FROM ENVIRONMENTAL THREATS:

- Data base destroyed by power surge.
- Data base damaged by exposing storage media to extreme humidity.
- Data base unavailable because air conditioning failure has shut system down.
- Sensitive data disclosed because power fluctuation caused a change in the security label of message thereby allowing its transmission to unauthorized sites.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SAMPLE IMPACTS OF
THREATS TO AND
VULNERABILITIES OF
COMMUNICATIONS**

STEP 4
**RESOURCE
TABLE
R4.4**

a. IMPACTS FROM NATURAL THREATS:

- Communication lines destroyed by earthquake
- Communication lines damaged by fallen tree during storm
- System use denied because of downed communication lines
- Sensitive material disclosed because cryptographic devices are found by unauthorized personnel

b. IMPACTS FROM INTENTIONAL HUMAN THREATS:

- Communication lines are destroyed by bomb explosion
- Communication lines are damaged by rioters
- Use of communication lines denied because a saboteur has cut the lines
- Sensitive information disclosed as a result of wiretaps

c. IMPACTS FROM UNINTENTIONAL HUMAN THREATS:

- Communication lines damaged by worker neglect when performing facility repairs
- Communication equipment destroyed by employee spilling a cleaning agent on equipment
- Use of communications equipment denied because communications security equipment is improperly keyed
- Sensitive data disclosed because crypto keying material was left in an opened security container.

d. IMPACTS FROM ENVIRONMENTAL THREATS:

- Communications equipment destroyed by water from overhead sprinkler system
- Communications equipment damaged by excessive humidity
- Use of communications equipment denied because facility becomes inaccessible due to structural problems
- Sensitive data disclosed because emergency personnel must clear the area after roof collapses.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SAMPLE IMPACTS OF
THREATS TO AND
VULNERABILITIES OF
COMPUTER HARDWARE**

STEP 4

**RESOURCE
TABLE
R4.5a**

a. IMPACTS FROM NATURAL THREATS:

- Central processing unit, peripherals, storage media damaged from exposure to water, debris, pollutants
- Magnetic media destroyed by fire
- Sensitive information disclosed because storage media is scattered throughout uncontrolled access areas
- System use denied because of damaged hardware, destroyed magnetic media, and inaccessible computer facility.

b. IMPACTS FROM INTENTIONAL HUMAN THREATS:

- System use denied because equipment was stolen and computer center was vandalized
- Hardware and computer center destroyed by arsonist attack
- Storage media damaged through negligent handling
- Sensitive information disclosed by unauthorized access.

c. IMPACTS FROM UNINTENTIONAL HUMAN THREATS:

- Peripheral equipment damaged by disk head crash
- Storage media destroyed by accidentally spilling coffee on the media
- Classified information disclosed through release of malfunctioning storage media to maintenance personnel prior to degaussing
- Use of hardware denied because operator failed to follow proper start-up procedures.

d. IMPACTS FROM ENVIRONMENTAL THREATS:

- Use of hardware denied because of overheating problems caused by failure of cooling system
- Hardware destroyed from water exposure caused by a break in an overhead water pipe
- Some peripheral equipment damaged by collapsing ceiling tiles
- Sensitive information disclosed because computer center is evacuated because of imminent structural failure and access by emergency personnel.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SAMPLE IMPACTS OF
THREATS TO AND
VULNERABILITIES OF
COMPUTER SOFTWARE**

STEP 4
**RESOURCE
TABLE
R4.5b**

a. IMPACTS FROM NATURAL THREATS:

- Software documentation and storage media destroyed by fire
- Software damaged from water and debris
- Sensitive information disclosed because sensitive software media is scattered throughout uncontrolled access areas
- Use of software denied because operational copies of software are damaged by water debris.

b. IMPACTS FROM INTENTIONAL HUMAN THREATS:

- Software is destroyed because of a trap door that was undetected because of poor configuration management procedures
- Software is damaged through neglect in handling and storage
- Software use denied because a virus caused erasure
- Sensitive information disclosed because an unauthorized user masqueraded as a legitimate user.

c. IMPACTS FROM UNINTENTIONAL HUMAN THREATS:

- Software is damaged because operator failed to write protect media
- Software is destroyed by accidentally deleting the program
- Sensitive information disclosed as a result of programming error which causes sensitive data to be misrouted to unauthorized output device.
- Software use denied because of program loading problems.

d. IMPACTS FROM ENVIRONMENTAL THREATS:

- Use of software denied because of power outage
- Software destroyed by water as a result of a break in an overhead water pipe
- Software damaged by surge in power
- Sensitive information disclosed because software was accessible by unauthorized personnel repairing structural defects.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SAMPLE IMPACTS OF
THREATS TO AND
VULNERABILITIES OF
ADP SYSTEM
PROCEDURES,
ADMINISTRATION AND
MANAGEMENT**

STEP 4

**RESOURCE
TABLE
R4.6**

a. IMPACTS FROM NATURAL THREATS:

- ADP center's contingency plan has never been tested, so recovery from destruction caused by a major flood is very slow.
- Absence of life-cycle configuration documentation hampers the task of rebuilding the damaged system.
- Sensitive information disclosed because tornado has scattered material throughout uncontrolled access area.

b. IMPACTS FROM INTENTIONAL HUMAN THREATS:

- System documentation is destroyed by arsonist attack.
- System documentation is damaged because vandals have maliciously shredded all manuals.
- Carelessness in protecting recent security test and evaluation results lead to their theft by campus hackers.

c. IMPACTS FROM UNINTENTIONAL HUMAN THREATS:

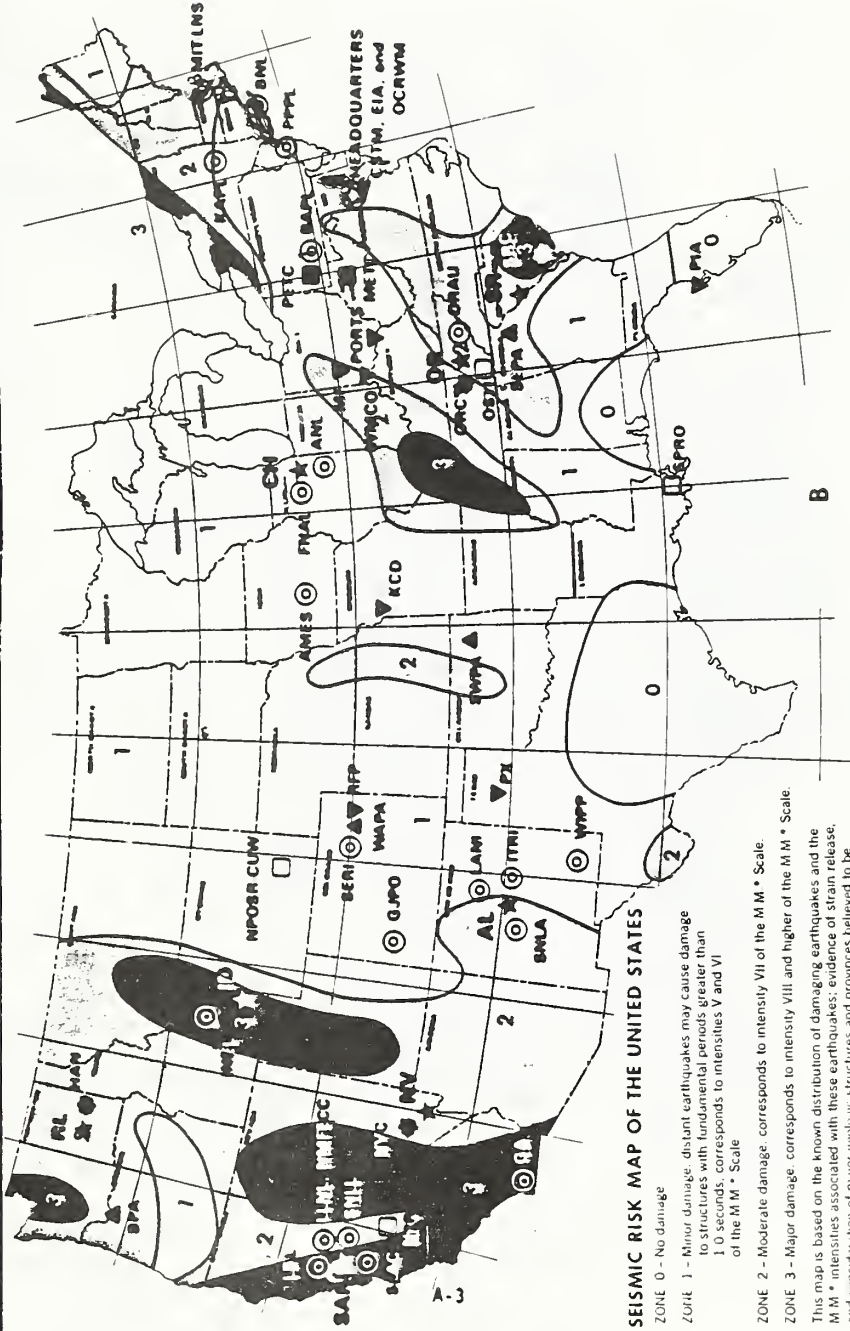
- Inattention to basic housekeeping procedures leads to serious system malfunction caused by dust and debris entering the system.

d. IMPACTS FROM ENVIRONMENTAL THREATS:

- Documentation is damaged because of extreme humidity.
- Routine maintenance checks of sprinkler system are neglected after staff reductions occur, leading to a costly repair.

ENVIRONMENTAL THREATS:
DATA ON
U.S. EARTHQUAKE ACTIVITY

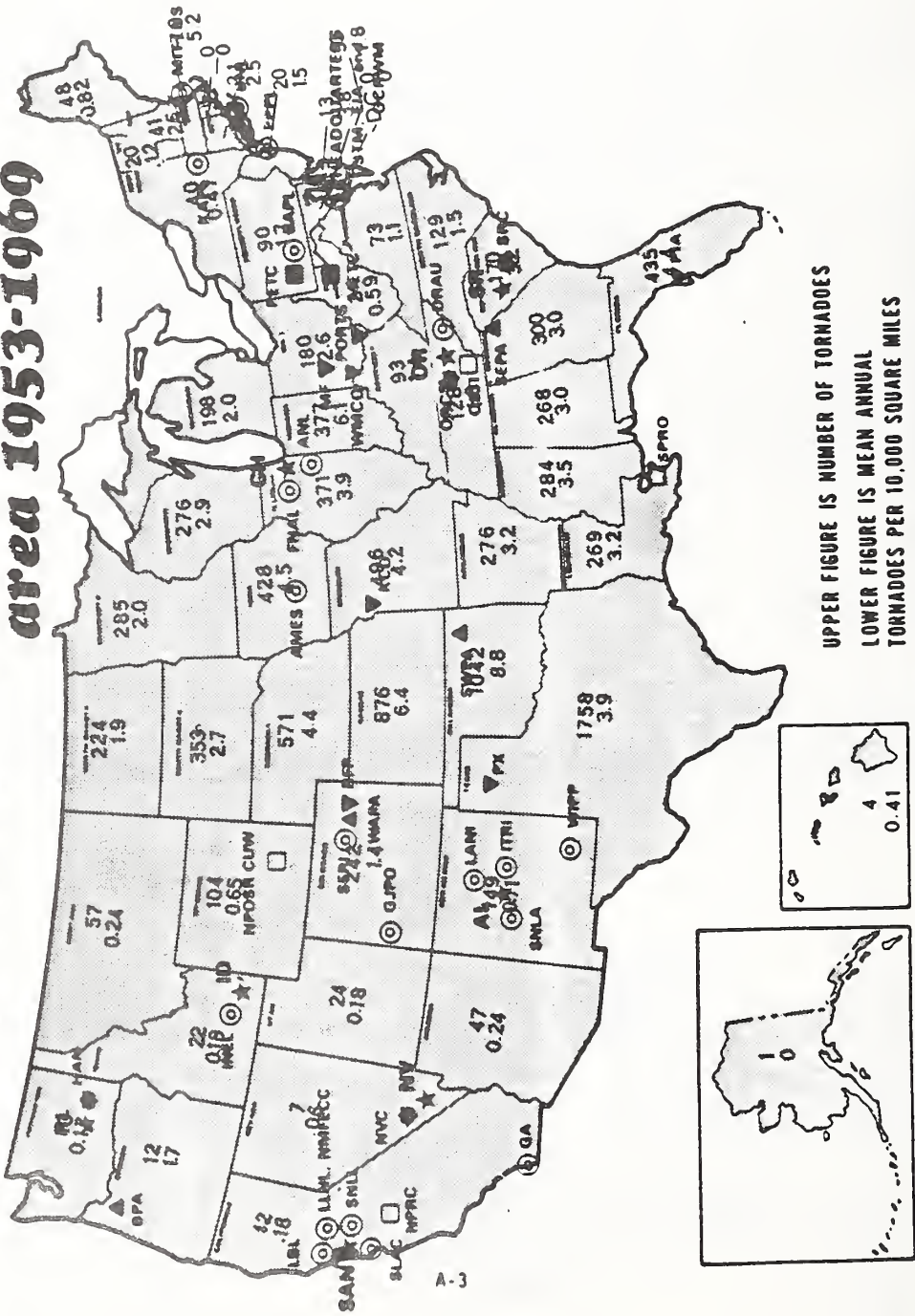
DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT



ENVIRONMENTAL THREATS: DATA ON U.S. TORNADO ACTIVITY

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT

tornado incidence by state and area 1953-1969



UPPER FIGURE IS NUMBER OF TORNADES
LOWER FIGURE IS MEAN ANNUAL
TORNADES PER 10,000 SQUARE MILES

NOTE: AS OF MAY 1989, THIS WAS THE MOST UP-TO-DATE MAP AVAILABLE OF U.S. TORNADO ACTIVITY.

ENVIRONMENTAL THREATS:
DATA ON
U.S. THUNDERSTORM ACTIVITY

DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT

THUNDERSTORM DAYS



Lightning is the attendant of thunderstorms. The map at left shows the incidence of thunderstorm days—days on which thunderstorms are observed—for the United States.

Alaska and Hawaii are less than 10.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**LEGEND FOR
MAP OF DOE FACILITIES
IN THE U.S.**

STEP 4

**RESOURCE
TABLE
R4.7d
(Page 2)**

⊙ HEADQUARTERS:

CSTM Computer Services and Tele-communications Management
EIA Energy Information Administration
OCRWM Office of Civilian Radioactive Waste Management

★ OPERATIONS OFFICES:

AL Albuquerque
CH Chicago
ID Idaho
NV Nevada
OR Oak Ridge
RL Richland
SAN San Francisco
SR Savannah River

■ ENERGY TECHNOLOGY CENTERS:

METC Morgantown
PETC Pittsburgh

▲ POWER ADMINISTRATIONS:

APA Alaska
BPA Bonneville
SEPA Southeastern
SWPA Southwestern
MAPA Western Area

⊙ COMPLEXES: (Generally, a complex includes an operations office and one or more research, test, and/or production facilities that are government-owned and contractor-operated.)

HAN Hanford
NVC Nevada
ORC Oak Ridge
SRC Savannah River

▼ PRODUCTION FACILITIES:

KCD Kansas City Plant
MF Mound Facility
PX Pantex Plant
PIA Pinellas Plant
PORTS Portsmouth Ohio Enrichment Facility
RFP Rocky Flats Plant
WACO Westinghouse Materials Company of Ohio

⊙ RESEARCH AND DEVELOPMENT FACILITIES

AMES Ames Laboratory
ANL Argonne National Laboratory
BAPL Bettis Atomic Power Laboratory
BNL Brookhaven National Laboratory
FNAL Fermi National Accelerator Laboratory
GA GA Technologies, Inc.
GJPO Grand Junction Project Office
INEL Idaho National Engineering Laboratory
ITRI Inhalation Toxicology Research Institute
KAPL Knolls Atomic Power Laboratory
LBL Lawrence Berkeley Laboratory
LLNL Lawrence Livermore National Laboratory
LANL Los Alamos National Laboratory
MIT-LNS Massachusetts Institute of Technology - Laboratory for Nuclear Science
NMFECC National Magnetic Fusion Energy Computing Center
ORAU Oak Ridge Associated Universities
PPPL Princeton Plasma Physics Laboratory
SNLA Sandia National Laboratories, Albuquerque
SNLL Sandia National Laboratories, Livermore
SERI Solar Energy Research Institute
SLAC Stanford Linear Accelerator Center
WIPP Waste Isolation Pilot Plant

□ OTHER DEPARTMENTAL COMPONENTS:

NPOSR-CUW Naval Petroleum and Oil Shale Reserves in Colorado, Utah, and Wyoming
NPRC Naval Petroleum Reserves in California
OSTI Office of Scientific and Technical Information
SPRO Strategic Petroleum Reserve Project Management Office

STEP 5



REVIEW AND SELECT COUNTERMEASURES OR
ACCEPT CURRENT RISK PROFILE
STEP 5

GENERAL PURPOSE OF STEP 5: The purpose of Step 5 is two-fold. It provides an opportunity to review available countermeasures in each of the security discipline areas and decide which ones are appropriate for implementation to counter the threat impacts identified in Step 4. However, if your review of threat impacts does not result in the identification of any new concerns, and confirms that your security program fully address the possible threats for your system and site, then Step 5 also allows you to acknowledge this by accepting your current risk profile in each or all of the security discipline areas.

STEP 5 END-PRODUCTS: This step will result in (1) a prioritized list of countermeasures for implementation in each of the security discipline areas; OR (2) a formal acceptance of your current risk profile made based on a documented review and analysis of possible threat impacts to your system.

IT IS RECOMMENDED THAT YOU REVIEW STEP 5 IN ITS ENTIRETY BEFORE STARTING. IF YOU ALREADY HAVE INFORMATION THAT FULFILLS THE OBJECTIVES OF STEP 5, AND/OR PREFER TO DEVELOP IT USING AN ALTERNATE RISK ASSESSMENT METHOD, YOU MAY PROCEED TO THE EXECUTIVE SUMMARY AND COMPLETE THE BLOCK FOR STEP 5. BE SURE TO NOTE WHAT SOURCES AND/OR METHODS WERE USED TO DEVELOP THIS INFORMATION. ATTACH COPIES OF ANY SUPPORTING DOCUMENTATION TO ENSURE THAT THE INFORMATION ENTERED ON YOUR EXECUTIVE SUMMARY IS FULLY SUPPORTED.

GETTING STARTED

1. Open to your copy of the Executive Summary and the Step 5 Worksheet in Volume II. The Step 5 Worksheet is located at the Step 5 Worksheet tab. Note the similarities between the Executive Summary, Step 5 Block and the Step 5 Worksheet. If you would like to record the results of your countermeasures review directly on the Executive Summary, Step 5 Block, you may. Otherwise, use the Worksheet provided as a strawman, first-cut version.

2. Familiarize yourself with the Step 5 Resource Tables R5.1a - R5.1h, Countermeasures Guidance. Note that there is a Resource Table that provides countermeasures guidance for each of the 8 security discipline areas listed in column (a) of the Step 5 Worksheet. A brief review of these 8 Resource Tables by individual discipline area is provided below:

-Resource Table R5.1a, Countermeasures Guidance for Physical Security: This table provides countermeasures for controlling access to and protecting the physical building, computing area/room, computing resources, support items, storage areas, and all human resources.

-Resource Table R5.1b, Countermeasures Guidance for Personnel Security: This table provides countermeasures for ensuring that personnel access to and use of computing resources (hardware, software, data) is properly controlled.

-Resource Table R5.1c, Countermeasures Guidance for Information Security: This table provides countermeasures for the protection of all hard-copy (non-electronic) information.

-Resource Table R5.1d, Countermeasures Guidance for Communications: This table provides countermeasures for the protection of all communications equipment, interfaces (wires, cables, lines, etc.), and the data transmitted on/by them in support of ADP processing/operations.

-Resource Table R5.1e, Countermeasures for Emissions Security (TEMPEST): This table provides countermeasures for the protection (from interception) of any emissions (signals, data) produced by electronic (ADP) systems.

-Resource Table R5.1f, Countermeasures for Computer Security: This table provides countermeasures for the protection of the total ADP system (hardware, software, and data).

-Resource Table R5.1g, Countermeasures for Administrative/Procedural Security and Security Management: This table provides countermeasures dealing with the establishment and management of a security organization and program necessary to support day-to-day operations while meeting security procedural requirements. (It should be noted that procedures specific to a security discipline area, such as procedures for configuration management or system testing, are set forth under the appropriate discipline (Computer Security in this example).

Resource Table R5.1h, Countermeasures for Environmental Security and Safety: This table provides countermeasures for ensuring that ADP resources and personnel are protected from environmental accidents, incidents, malfunctions, etc.

The countermeasures listed in the Step 5 Resource Tables are not intended to be all inclusive. The lists provide a fairly comprehensive treatment of the most prevalently used countermeasures in a specific security discipline area. Additional countermeasures guidance can be found by consulting the Guideline's Annotated Bibliography, Sections 5 and 6.

3. Keep in mind that countermeasures in one discipline area may actually protect assets in more than one area. For example, an administrative countermeasure may provide protection to communications assets, personnel, and the physical facility. Therefore, you should review all the countermeasures tables, not just the one in which you identified a vulnerability in Step 4.

4. The countermeasures listed in the Step 5 Resource Tables are organized, whenever possible, into common groupings (e.g., equipment-related, procedures, etc.). Note also that selected entries have a check mark next to them in the left hand margin. These check marks indicate that the particular countermeasure is generally easy to implement at a fairly low cost.

5. If any of the countermeasures listed in the Step 5 Resource Tables are unfamiliar, consult the Guideline's Glossary for clarification.

6. Finally, obtain any materials that already exist which may be helpful in completing this countermeasures review and selection, and/or which you may desire to use as supporting documentation for attachment to the Executive Summary. Helpful materials include countermeasures recommendations made in prior: Compliance Reviews, audits, security test and evaluation results, reports documenting the results of formal inspections and evaluations, Computer Security Program Reviews, and Management Reviews. Should any of these materials partially or fully meet the objectives of Step 5, document this on the Executive Summary and reference or append this documentation.

7. You may also find it useful to refer Resource Table R5.1i, Guidance for Determining Costs of Countermeasures, and to current issues of security-related product magazines and literature in order to develop approximate cost estimates for countermeasures. Your local security organization will most likely be able to provide you with product related information and associated cost estimates.

8. Proceed to Step 5, Worksheet W5, Countermeasures Review and Identification.

INSTRUCTIONS FOR
WORKSHEET W5, COUNTERMEASURES REVIEW AND IDENTIFICATION

GENERAL PURPOSE OF WORKSHEET W5: The purpose of this worksheet is to identify and select countermeasures appropriate for your system that are useful in countering or precluding the threat impacts identified in the previous Step. Further, it allows you to record the priority in which selected countermeasures should be implemented, to identify alternate approaches if such exist, and to provide an approximate cost for implementing the countermeasure (either a \$ estimate or an approximate amount of labor time required).

1. Complete Block 1 of the worksheet identifying your system.
2. Review the Step 5 Resource Tables (a - h) and place an "x" next to the countermeasures that would be useful in offsetting the threat impacts to a specific asset that you identified in Step 4. If you have determined that your current risk profile in each of the security discipline areas is acceptable and you choose not to implement further countermeasures, note "NONE" under column (a). Note also that in some cases, selected threats may persist regardless of the fact that perfectly appropriate countermeasures have already been implemented (e.g., accidents). For these cases, the response "NONE BEYOND THOSE IN-PLACE" should be recorded. For those discipline areas that you have identified necessary countermeasures to protect one or more assets, summarize your selections in the appropriate sections of the Countermeasures Review and Identification Worksheet, column (a). If there are several options available for countering a threat impact, or if a countermeasure provides benefits to more than one asset, note this on your worksheet as well.
3. After you have completed your countermeasures selection, develop approximate ("ballpark") costs for implementing the chosen countermeasures. The estimate may either be an approximate \$ amount or may reflect the approximate amount of labor time that would be required to implement the measure. Resource Table R5.1i provides general guidance on labor costs for your use in marking these estimates. For specific equipment items, refer to the security product literature to develop rough approximate costs. Enter the estimates in column (c), Approximate Cost.

When estimating the cost of countermeasures, keep in mind that if it was determined that the asset requires additional countermeasures, then the cost of the countermeasures does not have to be very precise for these purposes. The countermeasure cost has to be at least a reasonable amount LESS than the total estimated value of the asset. For example, an approximate \$1,000 expense to back-up a critical \$10,000 data base would be justified. It should be noted that the maximum acceptable cost of any countermeasure should be limited by the size of the expected losses which would be mitigated by that countermeasure.

4. After you have developed these general cost estimates, determine the priority order in which the countermeasures should be implemented. (Refer to the prioritization that you made in the Step 4, Threat and Vulnerability Review as guidance here to be sure the prioritization reflects your order of concern for the threat impacts that are identified there.) You may sequentially rank the order in which these countermeasures should be implemented (e.g., 1st, 2nd, 3rd, etc.) or you may again wish to use the following scheme:

- (1) = Fix immediately
- (2) = Fix within the next 6-12 months
- (3) = Fix if and when resources become available.

Enter your priorities in column (d) of the Worksheet and note the Target Date that each countermeasure should be in place in column (e).

5. After you have completed your countermeasures review and identification, it is again suggested that you convene a meeting of colleagues who are knowledgeable about the system and conversant with security matters. This informal meeting is suggested as a "sanity checkpoint" to discuss the results of your review in order to ensure completeness and provide different perspectives on the countermeasure selections made. (This type of meeting was also utilized in Step 4 to review and make final decisions regarding threat impacts. If desired, you may wish to review and select your countermeasures during this same forum.)

6. Summarize the results of Step 5 in the Step 5 Block of the Executive Summary. In column (a) note: whether you accept the current risk profile without implementation of any additional countermeasures (answer "Yes"); whether you accept the risk profile only with implementation of the countermeasures identified (answer "Yes IF"). If you still do not believe it is wise to accept the current risk profile for your system even WITH implementation of the countermeasures you identified, answer "NO" in column (a) of the Step 5 Block of the Executive Summary and explain why this is the case. Summarize the rest of your Worksheet's final results in columns (b), (c), (d), and (e).

7. Proceed to final Step 6 of the Guideline, Obtain Accountability: Management Understanding of Your Risk Profile and Countermeasures Required.

ACCESS CONTROL

- √ • Card entry system
- √ • Badging system
- √ • Locks
 - Padlocks
 - Cyphers (electronic; mechanical)
 - Combination
 - Key
- Fingerprint system
- Retinal scan system
- Voice print system
- Hand-geometry system
- √ • Restricted area sign
- √ • Access control lists
- Guard forces

INTRUSION DETECTION

- CCTV
- Alarms
- √
 - Balanced magnetic switches
 - Motion
 - Volumetric
 - Infrared

BARRIERS

- Perimeter fences
- Vehicle barricades
- √ • Security containers
- Vent/duct man barriers
- Brazed hinge pins
- √ • Facility construction (solid wood or metal doors; solid and slab-to-slab construction or equivalent walls; opening >96 square inches secured)

PROCEDURES

- √ • Visitor (includes delivery, maintenance personnel) access controls
 - Logs
 - Authorizations
 - Supervision (escorts)
- √ • Lock up procedures
- √ • After duty hour access controls
- √ • Emergency response procedures
- √ • Access control procedures
- √ • Security container use
- √ • Inventory, accountability, safeguarding keys, locks, badges, etc.
- √ • Security violation reporting
- √ • Security Officer
- √ • Security awareness education and training
- √ • Searches and inspections

- √ • Initial and continued screening and evaluation
- Training
 - √ - Operational
 - √ - Security awareness
 - √ - Cross training
- Security clearance
- √ • Separation of duties
- √ • Open-door policy

- Procedures for:
 - Identifying sensitive data/information
 - Assigning sensitivity levels
 - Marking and labeling data/information
 - Handling and storing data/information (i.e., a closed storage policy)
 - Dissemination data/information
 - Destroying data/information (to include all non-clearable media)
 - Limiting access to back-up files
 - Preparing contingency plan for loss of back-up data
 - Verifying accuracy of information
- Classification Guides
- Access Controls
 - Security containers
 - File cabinets
 - Cover sheets

- Protected distribution system
- End-to-End encryption
- Link encryption
- Key management
- √ • Error detection and recovery
 - Parity checks or checksums
 - Error correcting codes
- √ • Event handling and recovery
- √ • Backup and redundancy
- Dial-back modems
- √ • Configuration management
- √ • Patching procedures
- Handshaking
- Liveness checks
- Noise filters
- Synchronized clocks
- Trusted network interface
- Timestamping
- Traffic padding
- Choke packets
- Community of interest separation
- Crosscheck or summary reconciliation
- √ • Fault detection, isolation and tolerance
- √ • Flow/routing control
- Digital signatures
- Notarization
- Priority indicator
- Security guard mechanism
- Sequence numbering

NOTE: See the Glossary for explanation of countermeasures.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**COUNTERMEASURES
GUIDANCE:
EMISSIONS SECURITY
(TEMPEST)**

STEP 5

**RESOURCE
TABLE
R5.1e**

- TEMPEST Certified Equipment
- Physical Control Zone
- RED/BLACK Engineering
 - √ - Separation of lines
 - √ - Separation of equipment
- TEMPEST Tests and Inspections
- Filters
- Fiber Optic Cabling
- Shielding
 - Building
 - Equipment
 - Cables
 - Room

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**COUNTERMEASURES
GUIDANCE:
COMPUTER SECURITY**

STEP 5

**RESOURCE
TABLE
R5.1f**

SOFTWARE

- | | |
|--|--|
| <ul style="list-style-type: none"> √ • Security policy • Identification and authentication √ - Log on identification √ - Passwords - Smart cards - Retinal scans - Hand geometry scans - Keys - Voice prints - Digital signatures - Encryption - Access control lists • Accountability of equipment, software and data √ • Log-on attempts restricted • Automatic terminal time-outs √ • Audit trail records and reviews • Security software packages • Security labels • Memory and data/file/program storage protection - Base and bounds registers - Magnet detecting equipment √ - Locks and keys - Tagged memory √ - Declassification and clearing - Degausser √ - Backup √ - Backup storage on and off site √ - Secure storage for master copies - Data validation and integrity checks* - Encrypt files √ - File access restrictions | <ul style="list-style-type: none"> • Configuration Management √ - Software change authorization process √ - Structured design and programming √ - Software evaluation and testing of new and modified software • System alarms • Access Controls - Programs - Data - Documentation • Domain isolation • Penetration analysis and testing √ • Recovery management • Test and production software and data separation • Security kernel • Procedures - Backup - Declassifying and clearing - Destruction of classified material - Media marking, accountability, inventorying, handling, storing - Input and output controls - Certification - Software documentation - Password management/password changes - Tape and disk cleaning - Smoking, eating and drinking restrictions |
|--|--|

HARDWARE

- | | |
|---|--|
| <ul style="list-style-type: none"> • Chain of custody controls • Device identification √ • Backup and redundancy √ • Configuration management √ • Contingency planning √ • Console log √ • Interrupt handling • Lock-down devices √ • Access controls √ • Grounding | <ul style="list-style-type: none"> √ • Recovery management √ • Fault detection, isolation tolerance • Hardware protocol verification √ • Execution domains • Procedures - Shutdown and restart procedures - Preventive maintenance - Reconfiguration |
|---|--|

- √ • Separation of duties
- Standard operating procedures
- √ - Security incidents
- √ - Facility and system access controls
- √ - System operation
- √ - Backup
- √ - Emergency response
- √ - Housekeeping
- √ • Risk management
- √ • Contingency planning
- √ • Security tests and evaluations
- Certification
- Accreditation
- √ • Open door policy
- Establishment of computer security organization
- Designation of officials with specific duties and responsibilities
- Recovery management

- Power protectors
 - √ - Uninterrupted power supply
 - √ - Surge protectors
 - √ - Power plant physical security
 - √ - Emergency lighting
 - √ - Grounding (equipment and floor mats)
 - √ - Power off control switch

- Fire protection
 - √ - Fire detectors
 - √ - Fire suppression system
 - √ - Portable fire extinguishers
 - √ - Fire dampers in duct work
 - √ - Fire rated walls and partitions
 - √ - Noncombustible construction materials and furnishings
 - √ - Smoke exhaust systems
 - √ - Fire fighting teams

- Water protection
 - √ - Water drains
 - √ - Water sensors
 - √ - Humidity recording device and sensors
 - √ - Plastic sheeting for equipment

- Procedural
 - √ - Good housekeeping
 - √ - Emergency evacuation
 - √ - Environmental system preventative maintenance

- √ • Temperature recording device and sensors

- Anti-static carpeting

- Dust covers and filters

- √ • Building code compliance

- For Prices of "Off-the-Shelf" Security Products:
 - Consult security products catalogs and advertisements, as well as government price schedules and local vendor price lists available from your organization's Procurement and/or Security Office

-
- For Labor Costs:
 - Develop the total cost by multiplying approx. hours spent times labor cost per hour. Accepted labor costs for your use are provided:
 - Clerical: \$5-10/hr.
 - Junlor Professional or Programmer: \$15-20/hr.
 - Senlor Professional or Programmer: \$20-30/hr.

-
- Approximate no. of work hours per:
(Holidays and weekends are not included)
 - 1 Year: 2,080
 - 6 Months: 1,040
 - 1 Month: 170



STEP 6



OBTAIN ACCOUNTABILITY:
MANAGEMENT UNDERSTANDING OF RISK PROFILE AND COUNTERMEASURES REQUIRED
STEP 6

GENERAL PURPOSE OF STEP 6: Step 6 is the final step in the risk assessment process. It is a highly critical step, one that is often overlooked or neglected. The purpose of Step 6 is to provide management with an understanding of and obtain their accountability for the decisions and choices made throughout the risk assessment process. It provides a mechanism for reviewing the risk assessment results with management and discussing resource requirements for implementing the countermeasures identified.

STEP 6 END-PRODUCTS: There are no worksheets for final Step 6. The Executive Summary Block for Step 6, Management Understanding of Risk and Countermeasures Required, provides a sign-off area for your management to review the results of the risk assessment, and accept the current risk profile. This sign-off is the final end-product.

1. Enter your name on the line provided in the text of the Block 6 paragraph (at "Your Name") indicating that you performed the risk assessment, and enter the system for which the risk assessment was performed (at "system").
2. Present the results of the risk assessment to your management, using the Executive Summary pages to streamline the review and sign-off process. Use the Executive Summary pages to develop a management briefing to describe risks, to present upgrade recommendations, and to reach consensus on dollar requirements and implementation timetables.
3. Upon completion of the management review, obtain the required sign-off signatures. For the Unclassified Computer Security Program, sign-off is required by the Computer Protection Program Manager. For the Classified Computer Security Program, sign-off is required by the Computer Security Site Manager and, as appropriate, the Computer Security Operations Manager.



COMPLETED SAMPLE



GENERAL INFORMATION

The Center is located in a one story cement building inside a fenced compound. The compound itself has a guard at the main entrance of the south parking lot. All visitors are required to register with the receptionist located in the main lobby. Information on all visitors is entered into a database. A visitor is given a badge and is escorted from one building to another by assigned personnel. Upon leaving, the visitor must sign out and return the badge.

Access to the computer room itself is limited to the operators, system managers who are employed by the site contractor, and several individuals from the Information Systems Management Division. All janitorial services to the computer room are performed during the work day when an operator is on duty. To enter the computer room, authorized personnel must go through a card access system. Authorization for entry into the computer room is controlled by DOE personnel.

There is one major user entrance to the computing facility. All users have free access to the user's area 24 hours a day. The computer room is manned five days a week from 7:30 a.m. till 4:30 p.m. Security personnel monitor the computer room during periods when the computer room is not manned.

The facility processes sensitive/unclassified data. The creation and use of classified software and data is not authorized on any computer.



EXECUTIVE SUMMARY



1a. GEOGRAPHIC AND ADMINISTRATIVE INFORMATION

System Name/Identification: Anonymous DOE Computer Center
 Organization/User: Information Systems Division
 DOE Facility Name: Sibert Labs Inc.
 Site/Location: Breault Building
 Facility Address: Disketteville, New Jersey
 CSSO or Person Performing Risk Assessment:
 Name: Roger Risk Location: AI Laboratory
 Organization: Communication's ADP Center Phone No.: (000) xxx-0000

1b. PRIMARY SYSTEM USE

- | | |
|---|---|
| <input type="checkbox"/> Academic/Research | <input type="checkbox"/> Scientific/Technical |
| <input checked="" type="checkbox"/> Administration Management | <input type="checkbox"/> Manufacturing/Production |
| <input type="checkbox"/> Engineering/Design | <input type="checkbox"/> Other |

1c. SYSTEM CONNECTIVITY

Stand Alone System: Network System:
 LAN: WAN:

 : Open
 : Closed

1d. TYPE OF SYSTEM

<input type="checkbox"/> SMALL/SIMPLE SYSTEM		<input checked="" type="checkbox"/> LARGE/COMPLEX SYSTEM	
<input type="checkbox"/> Memory Typewriter	<input type="checkbox"/> CAD/CAM/Graphics Workstation	<input type="checkbox"/> CAD/CAM/Graphics Workstation	<input type="checkbox"/> Super-Computer
<input type="checkbox"/> Word Processor	<input type="checkbox"/> Other: _____	<input checked="" type="checkbox"/> Mini-Computer	<input type="checkbox"/> Other: _____
<input type="checkbox"/> Personal Computer	_____	<input type="checkbox"/> Mainframe	_____
<input type="checkbox"/> Smart Terminal	_____		

1e. SUMMARY OF SYSTEM REPLACEMENT COSTS

Replacement Costs	Very Low	Low	Medium	High	Very High
(1) Hardware Cost:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(2) Software Cost:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(3) Data Cost:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(4) Total System Cost:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

1f. STATUS OF SYSTEM BACK-UPS

	YES: All Needed Back-ups Exist	NO: Back-ups Are Needed	Identify Additional Back-up Required:
• Software Back-ups	<input checked="" type="checkbox"/>	<input type="checkbox"/>	_____
• Data Back-ups	<input checked="" type="checkbox"/>	<input type="checkbox"/>	_____

STEP 1

2a. SENSITIVITY OR CLASSIFICATION OF SOFTWARE AND DATA

(1) SOFTWARE (APPLICATIONS, PROGRAMS):

<input type="checkbox"/> Unclassified	<input type="checkbox"/> Sensitive Unclassified If Applicable, Check: • Vital Records <input type="checkbox"/> • UCNI <input type="checkbox"/> • Privacy Act <input checked="" type="checkbox"/> • OOU* <input type="checkbox"/> • Other <input checked="" type="checkbox"/>	<input type="checkbox"/> Classified • Highest Level _____ • Applicable Categories (RD, FRD, NSI, PARD) _____ • Mode of Operation _____
80 %	20 %	0 %

(2) DATA:

<input type="checkbox"/> Unclassified	<input type="checkbox"/> Sensitive Unclassified If Applicable, Check: • Vital Records <input type="checkbox"/> • UCNI <input type="checkbox"/> • Privacy Act <input checked="" type="checkbox"/> • OOU* <input type="checkbox"/> • Other <input checked="" type="checkbox"/>	<input type="checkbox"/> Classified • Highest Level _____ • Applicable Categories (RD, FRD, NSI, PARD) _____
60 %	40 %	0 %

2b. OVERALL IMPORTANCE OF A SYSTEM, SOFTWARE, AND DATA

1. SYSTEM

	<u>Very Low</u>	<u>Low</u>	<u>Medium</u>	<u>High</u>	<u>Very High</u>
Number of Users:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Frequency of Use:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Impact If Unavailable:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

2. SOFTWARE

	<u>Very Low</u>	<u>Low</u>	<u>Medium</u>	<u>High</u>	<u>Very High</u>
Frequency of Use:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Impact If Unavailable:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note Additional Back-up Requirements:

3. DATA

	<u>Very Low</u>	<u>Low</u>	<u>Medium</u>	<u>High</u>	<u>Very High</u>
Frequency of Use:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Impact If Unavailable:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note Additional Back-up Requirements:

Possible future category.

3. BASELINE SECURITY REQUIREMENTS REVIEW

STEP 3

(1) BLSR BY SECURITY DISCIPLINE	(a) ALL RQMTS. MET	(b) NOTED DEFICIENCY(IES)	(c) WILL DO BY	(d) COMMENTS AND/OR SUPPLEMENTARY UPGRADES
a) Physical Security:	Yes			
b) Personnel Security:	Yes			
c) Information Security:	Yes			
d) Communications Security:	Yes			
e) Emissions Security (TEMPEST):	N/A			
f) Computer Security (Hardware and Software):	Yes			
g) Procedural/ Administrative Security and Security Management:	Yes			
h) Environmental Security and Safety:	No	Walls don't meet fire rating standards. Value of equipment exceeds limitation. Cables are bundled in too large a group. Paper supplies not in metal container.	N/A 12/89 2/90 11/89	Accepting risk When new room is available Scheduled for correction Purchase required

(2) Based on results of Step 1 and Step 2, are the measures in-place sufficient given:

Hardware and Software: Cost(s) Yes No

System Software and Data: Characteristics and Importance Yes No

1) Comments: _____

4. THREAT AND VULNERABILITY ANALYSIS REVIEW

SEP 4

(1) ASSET AREA	(a) THREATS AND VULNERABILITY(IES)	(b) PROBABILITY (H,M,L)	(c) PRIORITY OF CONCERN
a) Physical (Facility):	<i>Storms</i>	<i>H</i>	<i>1</i>
b) Personnel:	<i>Accidents</i> <i>Emotional, mental, health problem</i> <i>Sensitive data disclosure</i>	<i>M</i> <i>M</i> <i>H</i>	<i>1</i> <i>2</i> <i>1</i>
c) Information, Data, and Emissions:	<i>Lighting</i> <i>Power Fluctuations</i>	<i>H</i> <i>H</i>	<i>1</i> <i>1</i>
d) Communications:	<i>Sabotage</i> <i>Unauthorized access</i> <i>Accidents</i>	<i>M</i> <i>M</i> <i>M</i>	<i>3</i> <i>2</i> <i>1</i>
e) Computer (Hardware & Software):	<i>Lighting</i> <i>All environmental threats</i>	<i>H</i> <i>M</i>	<i>1</i> <i>1</i>
f) Procedures, Administration, and Management:	<i>Storms</i> <i>All environmental threats</i>	<i>M</i> <i>M</i>	<i>1</i> <i>1</i>
g) Environmental Security and Safety:	<i>Storms</i> <i>Fire</i>	<i>M</i> <i>L</i>	<i>1</i> <i>2</i>

5. COUNTERMEASURES IDENTIFICATIONS AND RISK PROFILE ACCEPTANCE

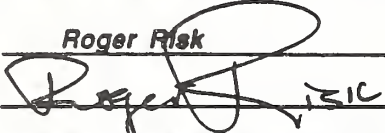
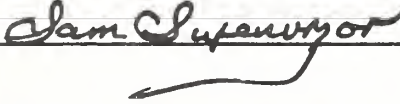
STEP 5

(1) SECURITY DISCIPLINE AREA	(a) ACCEPT CURRENT RISK PROFILE (YES OR NO)	(b) COUNTERMEASURES TO BE IMPLEMENTED	(c) PRIORITY	(d) APPROX. COST	(e) TARGET DATE
a) Physical Security:	Yes	None beyond those in place			
b) Personnel Security:	No	Establish procedures to notify supervisors of individual's clearance status	0	1	10/89
c) Information Security:	Yes	None beyond those in place			
d) Communications Security:	Yes	None beyond those in place			
e) Emissions Security (TEMPEST):	Yes	None beyond those in place			
f) Computer Security (Hardware and Software):	Yes	None beyond those in place			
g) Procedural/Administrative Security and Security Management	Yes	None beyond those in place			
h) Environmental Security and Safety:	No	Move equipment to new computer room	2	\$500	12/89
		Acquire metal containers for paper storage	1	\$350	11/89
		Reduce bundle size of cables	3	\$900	2/90

6. MANAGEMENT UNDERSTANDING OF RISK PROFILE AND COUNTERMEASURES REQUIRED

STEP 6

I/We have carefully assessed the risk(s) to the Anonymous DOE Computer Center system, its associated peripherals, (if applicable) its remote processing terminals, and telecommunications links. Based upon the assessment conducted by Roger Risk (your name), the implemented security measures and/or planned corrective measures are/will be sufficient to manage the risks identified for this system.

Name:	<u>Roger Risk</u>	Title:	<u>AI Lab Prog. Mgr.</u>
Signed:	<u></u>	Date:	<u>2/27/89</u>
Name:	<u>Sam Supervisor</u>	Title:	<u>AI Lab Chief</u>
Signed:	<u></u>	Date:	<u>2/29/89</u>

COMMENTS: _____

WORKSHEETS



1. System Name/identification: Anonymous DOE Computer Center
 Organization/User: Information Systems Division
 Primary Use: Scientific and technical R&D
 Location(s): Breault Bldg.; Disketteville, N.J.
 Date: 2/27/89

2. Connections:

Stand Alone System:

Network System:

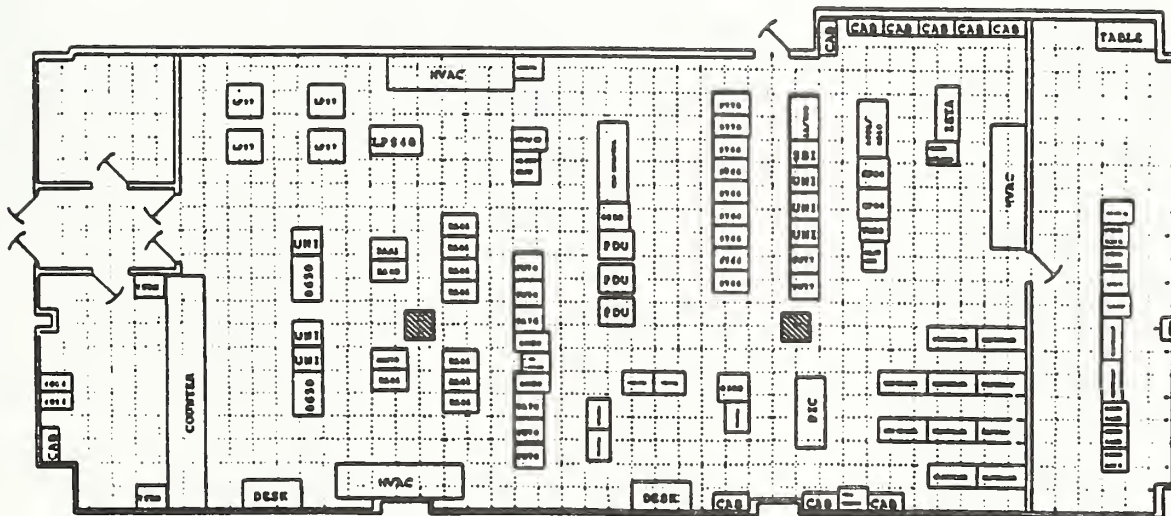
LAN: WAN:

: Open

: Closed

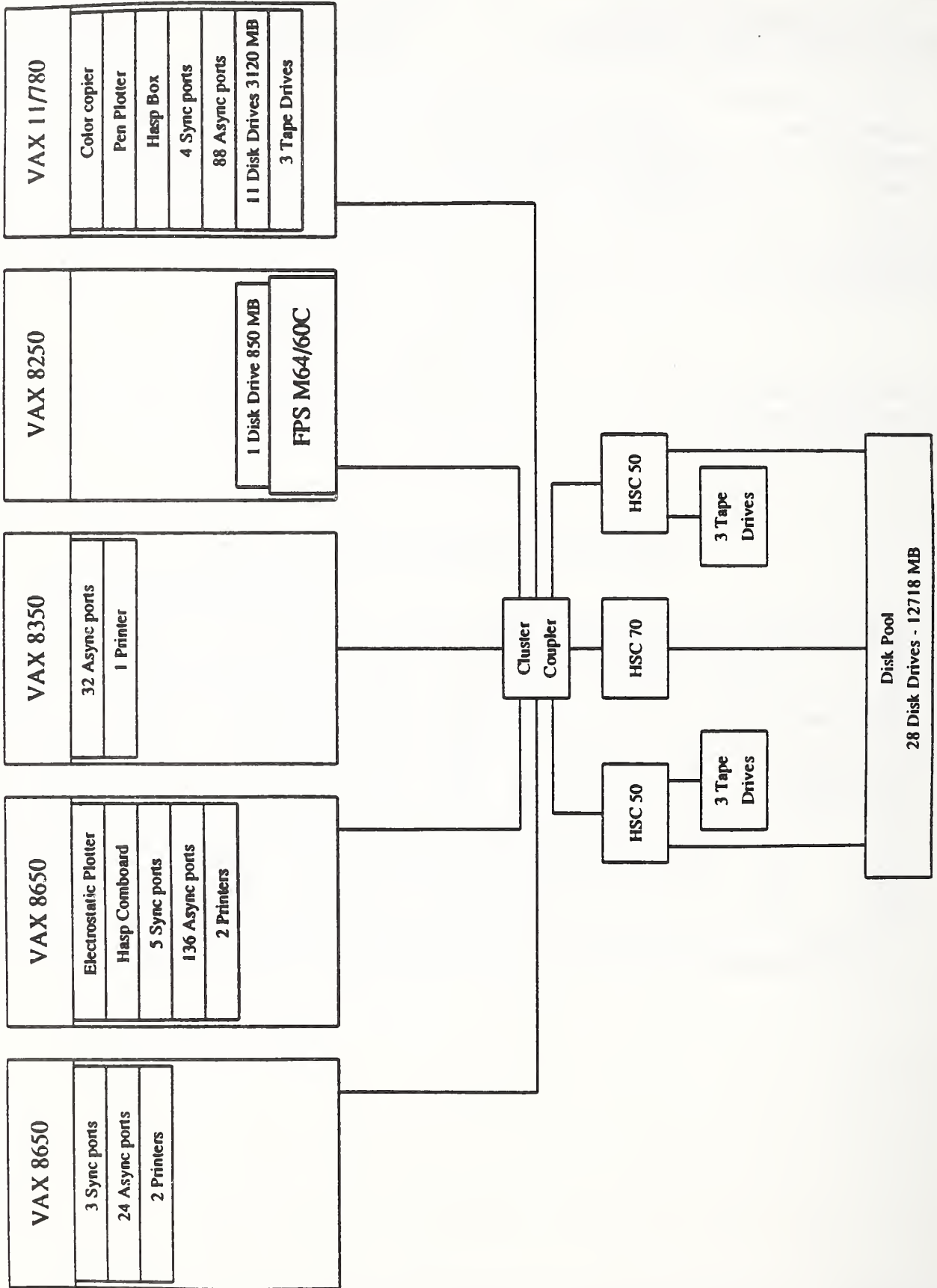
3. Configuration Diagram:

CENTRAL COMPUTER FACILITY



H-11

Computing Facility Configuration Diagram



**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**HARDWARE* INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.2a**

1. System Name/Identification: Anonymous DOE Computer Center
 Organization/User: Information Systems Division
 Primary Use: Scientific and technical R&D
 Location(s): Breault Building, Disketteville, N. J.
 Date: 2/27/89

2.		Hardware Inventory	Replacement Cost
(a) Ref. No.	Description/Identification	(b) \$ Amount OR	(c) Rating (VH-VL)
H. 1	2 VAX 8650's		VH
H. 2	1 VAX 8350		H
H. 3	1 VAX 8250		H
H. 4	1 VAX 11/780		H
H. 5	FPS M04/000		VH
H. 6	LPS40 LASER PRINTER		H
H. 7	4 LP27 LINE PRINTERS		H
H. 8	PI PLOTTER. 0448		H
H. 9	25 DISK DRIVES - 10898 MB		VH
H. 10	GANDALF		VH
H. 11	2 HSC 50's		H
H. 12	1 HSC 70		H
H. 13	6-9 track 1600/ ⁶²⁵⁰ BPI tape drives		VH
H. 14	5 DEC WRITER DISPLAY TERMINALS		L
H. 15	2 800/ ¹⁶⁰⁰ bpi tape drives		H
H. 16	1 4691 Color graphics copier		M

* Total Replacement Cost \$ _____ or VH Rating (VH, H, M, L, VL)

* NOTE: Hardware refers to the computer, peripherals, printer, and environmental and special support items.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**HARDWARE* INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.2b**

1. System Name/identification: Anonymous DOE Computer Center
 Organization/User: Information Systems Division
 Primary Use: Scientific and Technical R&D
 Location(s): Breactor Bldg. ; Dicketteville, N.J.
 Date: 2/27/89

2.		Hardware Inventory	Replacement Cost	
(a) Ref. No.	Description/Identification	(b) \$ Amount	OR	(c) Rating (VH-VL)
H. 17	GRAPHICS tablet			L
H. 18	NASP BOX			L
H. 19	2 VT220 terminals			VL
H. 20	LA 75 Printer			L
H. 21	tape cleaner verifier			H
H. 22	7 terminal servers DESRVB 200			H
H. 23	Communications EQUIP			VH
H. 24	4 modems			VL
H. 25	3 multiplexor			L
H. 26	Infetron 790 control system			M
H. 27	TUA 80 tape drives			M
H. 28	TRPO6 DISK DRIVES.			M
H. 29	Zetta plotter			M
H. 30	20 low speed modems			L
H. 31	LINE ANALYZER			L
H. 32	2 HARD COPY UNITS			VL

* Total Replacement Cost \$ See W1.2a or _____ Rating (VH, H, M, L, VL)

* NOTE: Hardware refers to the computer, peripherals, printer, and environmental and special support items.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**HARDWARE* INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.2C**

1. System Name/Identification: Anonymous DOE Computer Center
 Organization/User: Information Systems Division
 Primary Use: Scientific and Technical R&D
 Location(s): Breault Bldg.; Disketteville, D.S.
 Date: 2/27/89

2. Hardware Inventory		Replacement Cost	
(a) Ref. No.	Description/Identification	(b) Amount OR	(c) Rating (VH-VL)
H.33	2 4014 Tex. terminals		L
H.34	PAPER SHREDDER		L
H.35	LN03R laser printer		VL
H.36	OASIS laser pro printer		VL
H.37	AIR CONDITIONING UNITS		H
H.38	PERSONAL COMPUTER		L
H.			
H.			
H.			
H.			
H.			
H.			
H.			
H.			
H.			
H.			
H.			

3. Total Replacement Cost \$ See W1.2a or _____ Rating (VH, H, M, L, VL)

* NOTE: Hardware refers to the computer, peripherals, printer, and environmental and special support items.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SOFTWARE INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.3a**

1. System Name/Identification: Anonymous DOE Computer Center
 Organization/User: Information Systems Division
 Primary Use: Scientific and Technical R&D
 Location(s): Breault Bldg., Disketteville, N.J.
 Date: 2/27/89

(e) Ref. No.	(f) Description/Identification	(c) Type Storage Media	(d) Docs. & Backup Exist	(e) Approx. Hours to Develop	Replacement Cost	
					(f) \$ Amount	(g) OR Rating (VH-VL)
SW · 1	MAILING LABELS	b	yes	250		L
SW · 2	DRAFTING / DRAWING CONTROL SYSTEM	b	yes	250		L
SW · 3	ORAU PARTICIPANT TRACKING DATABASE	b	yes	600		M
SW · 4	TRAVEL PLAN SYSTEM	b	yes	780		M
SW · 5	SECURITY DATA SYSTEM	b	yes	154		L
SW · 6	TOTAL MAINTENANCE (HRL)	b	yes	N/A		
SW · 7	EMPLOYEE QUERY SYSTEM	b	yes	300		L
SW · 8	VISITORS REGISTRATION	b	yes	250		L
SW · 9	IN-HOUSE PAYROLL	b	yes	9583		VH
SW · 10	FACTSHEETS	b	yes	2375		H
SW · 11	PROJECT COST	b	yes	366		L
SW · 12	BIDDERS MAILING LIST	b	yes	375		L
SW · 13	INFORMATION CENTER REQUEST LOG SYSTEM	b	yes	40		VL
SW · 14	PERSONNEL REPORTING	b	yes	1975		H
SW · 15	MEDICAL DATA SYSTEM	b	yes	750		M

Total Replacement Cost \$ _____ or _____ M Rating (VH, H, M, L, VL)

* NOTE: Software includes all types of software, applications, and programs.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SOFTWARE INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.3b**

1. System Name/Identification: Anonymous DDF Computer Center
 Organization/User: Information Systems Division
 Primary Use: Scientific and technical R&D
 Location(s): Breault Bldg., Diketteville, N.J.
 Date: 7/27/89

(a) Ref. No.	(b) Description/Location	(c) Type Storage Media	(d) Does a Back-up Exist?	(e) Approx. Hours to Develop	(f) Replacement Cost	
					(f) Amount	(g) OR Rating (VH-VL)
SW-16	CONTRACT REPORT RECEIPT TRACKING	b	yes	375		L
SW-17	APPLICANT DATA BASE	b	yes	125		VL
SW-18	CONTRACT CLOSEOUTS	b	yes	250		L
SW-19	STORE ROOM INVENTORY	b	yes	2400		H
SW-20	MAINTENANCE MANAGEMENT (LMCS)	b	yes	750		M
SW-21	RIPA (OLD)	b	yes	250		L
SW-22	CONFERENCE REGISTRATION	b	yes	250		L
SW-23	ON-SITE PROPERTY MANAGEMENT SYSTEM	b	yes	733		M
SW-24	OFF-SITE PROPERTY MANAGEMENT SYSTEM	b	yes	500		M
SW-25	PROCUREMENT FORMS	b	yes	1000		M
SW-26	RIPA (NEW)	b	yes	583		M
SW-27	PHONE TRACKING SYSTEM	b	yes	250		L
SW-28	CADAS	b	yes	100		L
SW-29	MEETING & CONFERENCE MONITORING	b	yes	150		L
SW.						

1. Total Replacement Cost \$ See W1.3a or _____ Rating (VH, H, M, L, VL)

NOTE: Software includes all types of software, applications, and programs.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SOFTWARE * INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.3C**

1. System Name/Identification: Anonymous DOE Computer Center
 Organization/User: Information Systems Division
 Primary Use: Scientific and Technical R&D
 Location(s): Breault Bldg., Dixnotteville, N.J.
 Date: 2/27/89

2. Software Inventory		(c)	(d)	(e)	Replacement Cost	
(a) Ref. No.	(b) Description/Identification	Type Storage Media	Doc & Back-up Exist?	Approx. Hours to Develop	(f) Amount	(g) OR Rating (VH-VL)
SW-30	LIBRARY JOURNAL Catalog	b	yes	100		L
SW-31	TRAVEL PLAN (OLD)	b	yes	175		L
SW-32	VEHICLE MAINTENANCE	b	yes	320		L
SW-33	SOFTWARE INVENTORY SYS	b	yes	125		L
SW-34	SUPPLIES & MATERIALS	b	yes	120		VL
SW-35	CORRESPONDENCE & ACTION ITEM	b	yes	250		L
SW-36	DRUG FORMS	b	yes	125		L
SW-37	20/20 Spreadsheet	b	yes			pro prietary software - no replacem cost
SW-38	272 DICTED COMMUNICATIONS	b	yes			
SW-39	ADA	b	yes			
SW-40	BASIC	b	yes			
SW-41	BISS-32	b	yes			
SW-42	C	b	yes			
SW-43	COBOL	b	yes			
SW-44	CMS	b	yes			

Total Replacement Cost \$ See W1.3a or _____ Rating (VH, H, M, L, VL)

* NOTE: Software includes all types of software, applications, and programs.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SOFTWARE INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.3d**

1. System Name/Identification: Anonymous DOE Computer Center
 Organization/Users: Information Systems Division
 Primary Use: Scientific and technical R&D
 Location(s): Breactor Bldg. ? Disetteville, N.J.
 Date: 2/27/89

2. Software Inventory		(c)	(d)	(e)	Replacement Cost	
(a) Ref. No.	(b) Description/Identification	Type Storage Media	Does a Back-up Exist?	Approx. Hours to Develop	(f) \$ Amount	(g) Or Rating (VH-VL)
SW-45	CDD	b	yes			pr
SW-46	DRS	b	yes			opr.
SW-47	Data retrieve	b	yes			et
SW-48	Data Plot	b	yes			ary
SW-49	DECnet	b	yes			so
SW-50	Encryption Software	b	yes			ftw
SW-51	FMS	b	yes			are
SW-52	FORTRAN-77	b	yes			- no
SW-53	FORTRAN-LINT	b	yes			rep
SW-54	HASP COMMUNICATIONS	b	yes			lace
SW-55	IGL	b	yes			me
SW-56	IMSL	b	yes			nt
SW-57	LANGUAGE SENSITIVE EDITOR	b	yes			cost
SW-58	LISP	b	yes			
SW-59	MMS	b	yes			

Total Replacement Cost \$ See W1.3 a or _____ Rating (VH, H, M, L, VL)

* NOTE: Software includes all types of software, applications, and programs.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SOFTWARE INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.3e**

1. System Name/Identification: Anonymous DOE Computer Center
 Organization/User: Information Systems Division
 Primary Use: Scientific and Technical R&D
 Location(s): Breault Bldg., Disbetteville NJ.
 Date: 2/27/89

(a) Ref. No.	(b) Description/Identification	Software Inventory			Replacement Cost	
		(c) Type Storage Media	(d) Back-up Interval	(e) Approx. Hours to Develop	(f) \$ Amount	(g) Rating (VH-VL)
SW-60	NJE	b	yes			Pr
SW-61	NAG	b	yes			opr
SW-62	PDP-11 FORTRAN IV	b	yes			ret
SW-63	PL/I	b	yes			ary
SW-64	PLOT10	b	yes			so
SW-65	PACS+ EZLOG	b	yes			ft
SW-66	Rdb	b	yes			ware
SW-67	SPM	b	yes			- no
SW-68	SCA	b	yes			rep
SW-69	SMART-TAR	b	yes			lance
SW-70	SAS/SAS GRAPH	b	yes			me
SW-71	TDMS	b	yes			nt
SW-72	VMS OPERATING SYSTEM	b	yes			cost
SW-73	VPS-PLUS	b	yes			
SW-74	METALLIP	b	yes			

Total Replacement Cost \$ See W1.3a or _____ Rating (VH, H, M, L, VL)

* NOTE: Software includes all types of software, applications, and programs.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SOFTWARE INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.3f**

1. System Name/Identification: Anonymous DOE Computer Center
 Organization/Users: Information Systems Division
 Primary Use: Scientific and technical R&D
 Location(s): Breault Bldg., Disketteville N.J.
 Date: 2/27/89

(a) Ref. No.	(b) Description/Identification	(c) Type Storage Media	(d) Does a Backup Exist?	(e) Approx. Hours to Develop	Replacement Cost	
					(f) \$ Amount	(g) OR Rating (VM-VL)
SW-75	OVERHEAD	b	yes		proprietary software-	
SW-76	VIEWGRAPH	b	yes		No replacement cost	
SW .						
SW .						
SW .						
SW .						
SW .						
SW .						
SW .						
SW .						
SW .						
SW .						
SW .						
SW .						

Total Replacement Cost \$ See W1.3a or _____ Rating (VM, H, M, L, VL)

* NOTE: Software includes all types of software, applications, and programs.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**DATA INVENTORY
AND COST**

STEP 1
WORKSHEET
W1.4

1. System Name/Identification: Anonymous DOE Computer Center
 Organization/User: Information Systems Division
 Primary Use: Scientific and technical R&D
 Location(s): Bascalt Bldg.; D'Ketterville, N.S.
 Date: 3/27/89

(a) Ref. No.	(b) Description/Identification	(c) Approx. Hrs. to Develop	(d) Does a Back-up Exist?	Replacement Cost	
				(e) \$ Amount	(f) Rating (VH-VL)
D. 1	PERSONNEL DATA		YES		VH
D. 2	FINANCIAL DATA		YES		H
D. 3	SYSTEM DATA		YES		H
D. 4	INVENTORY DATA		YES		H
D. 5	TRACKING DATA		YES		H
D. 6	PLANNING DATA		YES		H
D. 7	PROCUREMENT DATA		YES		H
D. 8	PROJECTS		YES		H
D.					
D.					
D.					
D.					
D.					
D.					
D.					

Total Replacement Cost \$ _____ or H* Rating (VH, H, M, L, VL)

* NOTE: Data refers to data sets used as input for processing or that result from processing.

* - BASED ON NO BACKUPS EXISTING - 116-

DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT

SYSTEM
CHARACTERISTICS
AND IMPORTANCE

STEP 2
WORKSHEET
W2.1

(a) System *	(b) Number of Users (VL - VH)	(c) Frequency of Use (VL - VH)	(d) Impact if Unavailable (VL - VH)
System-1 Name/ID: <u>VAX</u> <u>Cluster</u>	75 + /VH	H to VH - The Cluster is used 24 hrs. a day, either interactively or through batch jobs.	H
System-2 Name/ID: <u>OFFICE</u> <u>AUTOMATION</u> <u>PC</u>	5 = VL	H - daily	H
System-3 Name/ID: _____ _____ _____			
System-4 Name/ID: _____ _____ _____			
System-5 Name/ID: _____ _____ _____			

NOTE: A system consists of the computer, peripherals, printer, environmental and other support items.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SOFTWARE
CHARACTERISTICS
AND IMPORTANCE**

**STEP 2
WORKSHEET
W2.2**

1. • System Name/Identification: Anonymous DOE Computer Center
 • Organization/User: Information Systems Division
 • Location(s): Brault Bldg.; Disketteville, D.S.
 • Date: 2/27/89

NOTE: Use reference numbers from Worksheet W1.3 to avoid retyping all entries.

2. Ref. No.	a) Software Sensitivity or Classification			b) Frequency of Use	c) Impact if Unavailable
	1) Unclassified?	2) Sensitive Unclassified? (Type)	3) Classified? (Note Level and Mode of Operation)		
SW - 1	✓			(H)	(M)
SW - 2	✓			(M)	(M)
SW - 3	✓			L	L
SW - 4	✓			(M)	(M)
SW - 5	✓			(H)	(M)
SW - 6	✓			VL	VL
SW - 7	✓			(M)	VL
SW - 8	✓			(H)	(M)
SW - 9		b) PRIVACY ACT INFO		(H)	(H)
SW - 10		F) DOE SECURITY OR MISSION RELATED		(H)	(M)
SW - 11	✓			L	L
SW - 12	✓			(M)	(M)
SW - 13	✓			(H)	(H)
SW - 14		b) PRIVACY ACT INFO		(M)	(M)
SW - 15		b) PRIVACY ACT INFO		(H)	(H)
3. Approx. %	<u>95</u> %	<u>5</u> %	<u> </u> %		

Software includes all types of software, applications, and programs.

** Total of columns 1, 2, and 3 should = 100% (reflecting all software (applications, programs) used).

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT

SOFTWARE * CHARACTERISTICS AND IMPORTANCE

STEP 2
WORKSHEET
W2.2.

1. • System Name/Identification: Anonymous DOE Computer Center
 • Organization/User: Information Systems Division
 • Location(s): Breault Bldg., Bisketteville, N.J.
 • Date: 2/27/89

NOTE: Use reference numbers from Worksheet W1.3 to avoid restating all entries.

2. Ref. No.	a) Software Sensitivity or Classification			b) Frequency of Use	c) Impact if Unavailable
	1) Unclassified?	2) Sensitive Unclassified? (Type)	3) Classified? (Note Level and Mode of Operation)		
SW-16	✓			(M)	(H)
SW-17		b) PRIVACY / ICT INFO		(M)	L
SW-18	✓			(M)	(M)
SW-19	✓			(H)	(M)
SW-20	✓			(H)	(M)
SW-21	✓			VL	VL
SW-22	✓			(M)	L
SW-23	✓			(H)	(M)
SW-24	✓			(M)	(M)
SW-25	✓			(M)	(M)
SW-26	✓			(H)	(M)
SW-27	✓			(M)	NE
SW-28		F) DOS SELECTION OR M.S. IS RELATED		(M)	(M)
SW-29	✓			VL	L
SW-30	✓			(M)	(M)
3. Apprx. %	<u>98</u> %	<u>2</u> %	<u> </u> %		

Software includes all types of software, applications, and programs.

** Total of columns 1, 2, and 3 should = 100% (reflecting all software (applications, programs) used).

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SOFTWARE
CHARACTERISTICS
AND IMPORTANCE**

**STEP 2
WORKSHEET
W2.2**

1. • System Name/Identification: Anonymous DOE Computer Center
 • Organization/User: Information Systems Division
 • Location(s): Brault Bldg. - Disketteville, N.J.
 • Date: 2/27/89

NOTE: Use reference numbers from Worksheet W1.3 to avoid retyping all entries.

2. Ref. No.	a) Software Sensitivity or Classification			b) Frequency of Use	c) Impact if Unavailable
	1) Unclassified?	2) Sensitive Unclassified? (Type)	3) Classified? (Note Level and Mode of Operation)		
SW - 31	✓			(M)	(M)
SW - 32	✓			VL	VL
SW - 33	✓			L	VL
SW - 34	✓			L	VL
SW - 35	✓			VL	VL
SW - 36	✓			L	L
SW - 37 thru 73 -		PROGRAMMING TOOLS		(H)	(M)
SW - 74	LIBRARY OF	FREQUENT CODE USED = 1		(H)	(M)
SW .					
SW .					
SW .					
SW .					
SW .					
SW .					
SW .					
SW .					
3. Approx. %	<u>80</u> %	<u>20</u> %	<u>0</u> %		

Software includes all types of software, applications, and programs.

** Total of columns 1, 2, and 3 should = 100% (reflecting all software (applications, programs) used).

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**DATA
CHARACTERISTICS
AND IMPORTANCE**

**STEP 2
WORKSHEET
W2.3**

1. System Name/Identification: Anonymous DOE Computer Center
 Organization/User: Information Systems Division
 Location(s): Breault Bldg.; Disketteville, N.S.
 Date: 2/27/89

NOTE: Use reference numbers from Worksheet W1.4 to avoid retyping all entries.

2. Ref. No.	(a) Data Sensitivity or Classification			b) Frequency of Use	c) Impact if Unavailable
	1) Unclassified?	2) Sensitive Unclassified? (Note Type)	3) Classified? (Note Level)		
D-1		b) PRIVACY ACT INFO		(H)	(H)
D-2	✓			(M)	(M)
D-3	✓			(H)	(M)
D-4	✓			(M)	(M)
D-5	✓			(M)	(M)
D-6	✓			(M)	(M)
D-7		f) DOE SEC OR MISSION REL		(M)	(M)
D-8		f) DOE SEC OR MISSION REL.		(M)	L
D.					
D.					
D.					
D.					
D.					
D.					
D.					
D.					
3. Approx. %	<u>60</u> %	<u>40</u> %	<u>0</u> %		

Data refers to specific data sets used as input for processing or that result from processing.
 ** Total of columns 1, 2, and 3 should = 100% of all data used.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
PHYSICAL SECURITY**

**STEP 3
WORKSHEET
W3.1a**

System Name/Identification: Anonymous DOE Computer Center

SENSITIVE UNCLASSIFIED

Y . STORE INFORMATION/DATA IN UNLOCKED FILES, DESKS WITHIN CONTROLLED/GUARDED AREA. (B)

Y . STORE INFORMATION/DATA IN LOCKED REPOSITORY IN UNCONTROLLED/GUARDED AREA. (B)

BOTH

Y . DEFINE PHYSICAL SECURITY REQUIREMENTS FOR ADP OPERATIONS AT ONSET OF PROGRAM. (D)

Y . UTILIZE A PERSONNEL IDENTIFICATION SYSTEM FOR FACILITY WITH 30+ INDIVIDUALS. (q, r, u)

Y . RECOVER BADGES OF TERMINATING EMPLOYEES AND DEPARTING VISITORS. (u)

Y . REPLACE BADGES AND PASSES AS APPROPRIATE. (u)

Y . RETAIN RECORD OF LOST BADGES, PASSES, CREDENTIALS, AND SHIELDS. (u)

Y . DESIGN ELECTRONIC ALARMS TO MEET SITE-SPECIFIC PROTECTION NEEDS AND REQUIREMENTS IN DOE 5632.5. (q)

Y . USE A RECEPTIONIST OR EMPLOYEE WITH ASSIGNED RESPONSIBILITY TO CONTROL ACCESS DURING WORKING HOURS. (r)

Y . MAINTAIN A VISITORS LOG. (r)

Y . POST TRESPASSING SIGNS AROUND PERIMETER AND ENTRANCES. (r)

Y . INSPECT AND SEARCH VEHICLES AND HAND CARRIED ITEMS RANDOMLY. (r)

Y . POST CONTRABAND/PROHIBITED ITEMS SIGN AT ALL ENTRANCES. (r)

Y . IMPEDE ACCESS WITH BARRIERS (I.E., WALLS, FENCES, ETC.). (r)

Y . LOCK AREA, BUILDING, ADP CENTER, ETC. WHEN UNOCCUPIED. (r)

Y . UTILIZE LOCKS THAT ARE GSA/GOVERNMENT APPROVED. (r)

Y . CONTROL AND ACCOUNT FOR ALL KEYS AND COMBINATIONS. (r)

Y . CHANGE LOCKS AND COMBINATIONS WHEN LOST/COMPROMISED. (r)

Y . PROVIDE INTRUSION DETECTION SYSTEM AS APPROPRIATE. (r)

Y . TEST AND MAINTAIN ALARM/SECURITY SYSTEMS AND COMPONENTS IN OPERABLE CONDITION. (r)

Y . ESTABLISH EMERGENCY PLANS. (r)

Y . DESIGN ELECTRONIC ALARMS TO MEET SITE-SPECIFIC PROTECTION NEEDS AND REQUIREMENTS WITH DOE ALARM REQUIREMENTS. (q)

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
PHYSICAL SECURITY**

STEP 3

WORKSHEET
W3.1b

System Name/Identification: Anonymous DOE Computer Center

CLASSIFIED

*N/A No classified data
is on Computer System*

- DETECT AND DETER UNAUTHORIZED ACCESS TO ADP CENTERS. (q)
- ESTABLISH SECURITY AREAS AS REQUIRED BY DOE BASED ON MISSION AND SIZE. (a)
- SAFEGUARD STOCK OF UNUSED BADGES, PASSES, CREDENTIALS, AND SHIELDS. (u)
- IDENTIFY SECURITY IMPORTANCE RATINGS OF SECURE FACILITIES. (m)
- CONTROL AND LIMIT ACCESS TO PERSONNEL WHO ARE CLEARED FOR ACCESS TO THE HIGHEST CLASSIFICATION LEVEL OF INFORMATION. (p, q)
- ESTABLISH A TSCM PROGRAM FOR FACILITIES THAT HOUSE CLASSIFIED ADP SYSTEMS. (o)
- NOTIFY RESPONSIBLE ORGANIZATION OF PHYSICAL SECURITY DEFICIENCIES. (m)
- CONDUCT INITIAL AND PERIODIC SECURITY SURVEYS TO ENSURE DOE SECURITY POLICIES AND PROCEDURES ARE IMPLEMENTED. (m)

Y: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
PERSONNEL SECURITY**

STEP 3

**WORKSHEET
W3.2**

System Name/Identification: Anonymous DOE Computer Center

SENSITIVE UNCLASSIFIED

Y	• LIMIT PERSONNEL ACCESS TO SENSITIVE UNCLASSIFIED MATERIALS VIA DISSEMINATION AND ACCESS CONTROLS. (B,E,F,H)
Y	• SCREEN ALL PERSONNEL INVOLVED WITH SENSITIVE DATA. (E)
Y	• REQUIRE PROOF OF IDENTITY TO RECEIPT FOR INFORMATION. (H)

CLASSIFIED

	• CONTROL AND LIMIT ACCESS TO CLASSIFIED INFORMATION TO AUTHORIZED PERSONNEL ONLY. (n, p)
	• LIMIT PERSONNEL ACCESS TO WEAPONS DATA MATERIALS VIA DISSEMINATION AND ACCESS CONTROLS. (v)
	• CONTROL ACCESS TO FOREIGN INTELLIGENCE INFORMATION. (x)
	• ENSURE PERSONNEL ARE COGNIZANT OF THEIR RESPONSIBILITIES TO SAFEGUARD AND CONTROL CLASSIFIED DOCUMENTS. (n)
	• OBTAIN NECESSARY VISITOR ACCESS AUTHORIZATIONS PRIOR TO PERMITTING ACCESS TO FACILITIES CONTAINING NAVAL NUCLEAR PROPULSION INFORMATION (NNPI). (h)
	• ENSURE THAT ALL INDIVIDUALS REQUIRING ACCESS TO CLASSIFIED MATERIAL ARE APPROPRIATELY CLEARED. (g)
	<i>N/A - No classified data on computer system</i>

Y: YES = Y NO = N NOT APPLICABLE = NA PARTIALLY = P

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT

REVIEW OF BASELINE SECURITY REQUIREMENTS FOR: INFORMATION SECURITY

STEP 3

WORKSHEET
W3.3

System Name/Identification: Anonymous DOE Computer Center

SENSITIVE UNCLASSIFIED

- | | |
|---|--|
| Y | • MAINTAIN CURRENT INVENTORY OF STORED INFORMATION. (A) |
| Y | • USE COVER SHEETS AND SPECIAL MARKINGS FOR UCNI. (B) |
| Y | • STORE UCNI MATERIALS IN LOCKED REPOSITORY. (B) |
| Y | • STORE UCNI MATERIALS IN UNLOCKED FILES AND DESKS IF WITHIN CONTROLLED/GUARDED AREA. (B) |
| Y | • SHRED OR BURN MEDIA TO BE DESTROYED. (B) |
| Y | • PROTECT COMPUTER SECURITY PROGRAM INFORMATION. (B,E) |
| Y | • REVIEW VITAL RECORDS ANNUALLY. (A) |
| Y | • APPROPRIATELY MARK ON THE COVER AND TITLE PAGE OF ALL SOFTWARE DOCUMENTATION FOR SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE WHICH MAY BE DISSEMINATED TO OTHERS. (J) |
| Y | • UTILIZE OPSEC TECHNIQUES OR MEASURES TO PROTECT CLASSIFIED OR SENSITIVE/UNCLASSIFIED INFORMATION. (K) |
| Y | • PREPARE AN OPSEC THREAT STATEMENT AND DEVELOP A CRITICAL AND SENSITIVE INFORMATION LIST AND SUPPORTING ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION. (K) |
| Y | • DEVELOP PROCEDURES FOR PROPERLY REPORTING, HANDLING, SAFEGUARDING, AND DISPOSING OF DOE SCIENTIFIC AND TECHNICAL INFORMATION. (I) |
| Y | • PROHIBIT DUPLICATION OF SOFTWARE, DATA FOR PERSONAL USE OR ON HOME COMPUTERS. (L) |

BOTH

- | | |
|-----|--|
| Y | • IDENTIFY ALL SENSITIVE DATA, INFORMATION, MATERIALS. (A,C,E,F) |
| Y | • DEFINE INFORMATION SECURITY NEEDS AT ONSET OF ALL PROGRAMS. (D) |
| Y | • REVIEW PROGRAMS AND DATA FOR COMPLIANCE WITH REQUIREMENTS FOR HANDLING AND CONTROL OF SENSITIVE DATA. (A,C,E,H) |
| N/A | • MARK SENSITIVE UNCLASSIFIED AND CLASSIFIED MATERIAL AND EQUIPMENT WITH NECESSARY MARKINGS EITHER BY STAMPING, TAGS, LABELS, OR OTHER SUITABLE MEANS. (q) |
| N/A | • STORE SENSITIVE OR CLASSIFIED MATTER IN SECURITY CONTAINERS. (q) <u>Locked file cabinets</u> |

CLASSIFIED

- | | |
|--|---|
| | • MAINTAIN ACCOUNTABILITY SYSTEM, AS APPROPRIATE, TO ACCOUNT FOR AND DETERMINE WHEN CLASSIFIED MATTER IS LOST OR UNACCOUNTED FOR. (a) |
| | • MARK CLASSIFIED MATERIAL, MEDIA, AND OTHER EQUIPMENT WITH CLASSIFICATION AND OTHER NECESSARY MARKINGS, EITHER BY STAMPING, TAGS, LABELS, OR OTHER SUITABLE MEANS. (q) |
| | • STORE CLASSIFIED MATTER IN APPROVED SECURITY CONTAINERS. (q) |
| | • CONDUCT ANNUAL REVIEW OF TOP SECRET DOCUMENTS. (n) |
| | • AFFIX SPECIAL HANDLING MARKINGS TO NNPI AS APPROPRIATE. (h)
<u>N/A - No classified information on computer system</u> |

YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
COMMUNICATIONS
SECURITY (COMSEC)**

STEP 3

WORKSHEET
W3.4

System Name/Identification: Anonymous DOE Computer Center

SENSITIVE UNCLASSIFIED

Y AS APPROPRIATE:

Y • USE OF PRIVACY DEVICES TO PROTECT UNCLASSIFIED INFORMATION. (c)

Y • USE OF DES TO PROTECT UNCLASSIFIED, SENSITIVE INFORMATION. (c)

BOTH

Y • PROCURE/USE CRYPTO GEAR FOR UNCLASSIFIED SENSITIVE DISCUSSIONS/TRANSMISSIONS, IF DEEMED NECESSARY. (c)

Y • DESIGN AND INSTALL PDS, AS APPROPRIATE. (d)

Y • SECURE CLASSIFIED AND UNCLASSIFIED SENSITIVE SYSTEMS TO PREVENT COMPROMISE OR EXPLOITATION. (c)

CLASSIFIED

• CONDUCT SECURITY SURVEYS OF SECURE COMMUNICATIONS CENTERS. (m)

• PROCURE/USE NSA APPROVED CRYPTOGRAPHIC DEVICES. (p)

• ENSURE CLASSIFIED INFORMATION IS NOT DISCUSSED OR TRANSMITTED OVER UNENCRYPTED OR NONSECURE TELEPHONE SYSTEMS. (n)

• PROCURE/USE CRYPTO GEAR FOR CLASSIFIED DISCUSSIONS/TRANSMISSIONS. (c)

N/A - No classified material is on computer system.

KEY: YES = Y NO = N NOT APPLICABLE = NA PARTIALLY = P

(1) NOTE: Additional PDS Guidance is provided in the DOE PDS Procedural Guide (u) (Confidential).

(2) NOTE: Additional COMSEC guidance regarding the role and responsibilities of the CRYPTO custodian are provided in the DOE COMSEC Procedural Guide. (v) (Confidential).

(3) NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
EMISSIONS SECURITY
(TEMPEST)**

STEP 3

WORKSHEET
W3.5

System Name/Identification: Anonymous DOE Computer Center

BOTH SENSITIVE UNCLASSIFIED/CLASSIFIED

AS APPROPRIATE:

- | | |
|-----|--|
| N/A | • APPOINT TEMPEST COORDINATOR. (b) |
| N/A | • PERFORM TEMPEST SURVEYS. (b) |
| N/A | • ZONE TEST EVERY 3 YEARS. (b) |
| N/A | • MAINTAIN TEMPEST FILE FOR EACH FACILITY. (b) |
| N/A | • COMPLY WITH EMISSIONS SECURITY REQUIREMENTS. (b) |

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

NOTE: Additional TEMPEST guidance is provided in the DOE TEMPEST Procedural Guide (u) (Confidential). As of May 1989, this guide was undergoing a major update/revision.

(2) NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT

REVIEW OF BASELINE SECURITY REQUIREMENTS FOR: COMPUTER SECURITY*

STEP 3

WORKSHEET
W3.6a

System Name/Identification: Anonymous DOE Computer Center

SENSITIVE UNCLASSIFIED

Y	• DEFINE OPERATING AND APPLICATION SOFTWARE SECURITY NEEDS AT ONSET OF PROGRAM. (D,E,H)
Y	• MAINTAIN ACCESS LOG(S) TO DETECT UNAUTHORIZED ACCESS ATTEMPTS. (E)
Y	• RANDOMLY REVIEW FILE CONTENTS. (E)
Y	• ESTABLISH CONFIGURATION MANAGEMENT CONTROLS TO TRACK HARDWARE AND SOFTWARE SECURITY UPGRADES BASED ON RESULTS OF RISK ASSESSMENT. (E)
Y	• DETERMINE IMPORTANCE OF APPLICATION TO MISSION. (E)
Y	• DEVELOP COMPUTER PROTECTION PLAN. (E)
Y	• ESTABLISH AND IMPLEMENT COMPUTER SECURITY CONTROL PROCEDURES TO PROTECT HARDWARE, SOFTWARE, AND DATA AGAINST THEFT, LOSS, UNAUTHORIZED MANIPULATION, FRAUDULENT ACTIVITIES AND NATURAL DISASTERS. (K)
Y	• ADVISE APPROPRIATE AUTHORITIES OF ANY SENSITIVE/UNCLASSIFIED COMPUTER SECURITY VULNERABILITY DETECTED IN THE COURSE OF AN OPSEC VULNERABILITY ASSESSMENT. (K)
Y	• ESTABLISH AND IMPLEMENT COMPUTER OPERATION CONTROL PROCEDURES TO ENSURE ACCURACY AND COMPLETENESS OF THE INFORMATION MAINTAINED AND PROCESSED. (K)
Y	• ESTABLISH, DOCUMENT, AND ENFORCE PROCEDURES FOR TESTING AND IMPLEMENTING SOFTWARE CHANGES (K)
Y	• ESTABLISH AND IMPLEMENT HARDWARE CONTROLS FOR ALL HARDWARE PROCUREMENT ACTIONS. (K)
Y	• ESTABLISH AND ENFORCE CONTROL PROCEDURES FOR DISTRIBUTED PROCESSING AND NETWORK OPERATIONS. (K)
Y	• REQUIRE THAT SYSTEM DESIGN, DEVELOPMENT, AND MODIFICATION CONTROL PROCEDURES PROVIDE ADEQUATE SEPARATION OF DUTIES AND ASSURES USER, MANAGEMENT, AND INTERNAL AUDITOR PARTICIPATION. (K)
Y	• ESTABLISH CONTROL MECHANISMS TO ENSURE THAT DATA REACHES THE COMPUTER APPLICATION WITHOUT LOSS, UNAUTHORIZED ADDITION OR MODIFICATION, OR OTHER ERROR. (K)
Y	• ESTABLISH AND ENFORCE PROCEDURES FOR CONVERTING AND ENTERING DATA THROUGH TERMINALS AND DETAIL THE PROCESS FOR IDENTIFYING, CORRECTING, AND REPROCESSING DATA REJECTED BY THE APPLICATION. (K)
Y	• DEVELOP, DOCUMENT AND IMPLEMENT CONTROL PROCEDURES FOR PROCESSING DATA AND SCHEDULING DATA PROCESSING. (K)
Y	• DEVELOP, DOCUMENT, AND IMPLEMENT OUTPUT CONTROL PROCEDURES. (K)
Y	• DEVELOP AND IMPLEMENT EFFECTIVE CONTROLS FOR THE ACQUISITION, OPERATION AND SECURITY OF MICROCOMPUTERS. (K)
Y	• REQUIRE WRITTEN AUTHORIZATION TO USE COMPUTER EQUIPMENT FOR OFF-SITE WORK. (L)

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

* Covers Hardware, Software, and Computer Security Related Procedures.

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
COMPUTER SECURITY ***

STEP 3

**WORKSHEET
W3.6b**

System Name/Identification: Anonymous DOE Computer Center

BOTH

- | | |
|---|--|
| Y | • PROVIDE CONFIGURATION MANAGEMENT CONTROLS. (C, E) |
| Y | • REVIEW/APPROVE AND CERTIFY DESIGN OF NEW OR CHANGED HARDWARE/SOFTWARE. (C,D,E,H) |
| Y | • DEFINE, EVALUATE, AND REEVALUATE SECURITY REQUIREMENTS THROUGHOUT SYSTEM LIFE-CYCLE. (C,D,E,H) |
| Y | • AUDIT SYSTEM. (C,E,p) |
| Y | • DEVELOP AND TEST CONTINGENCY PLAN, INCLUDING BACK-UP AND RECOVERY FEATURES. (A,C,p) |
| Y | • TEST HARDWARE AND SOFTWARE PROTECTIVE FEATURES. (E, p) |

CLASSIFIED

- | | |
|--|---|
| | • PREPARE ADP SECURITY PLAN. (p) |
| | • DEVELOP, IMPLEMENT, MAINTAIN, AND DOCUMENT ALL ADP SECURITY MEASURES. (p) |
| | • CLEAR AND SANITIZE ADP RESOURCES FOR CLASSIFIED PROCESSING. (p) |
| | • DEVELOP A CONTINGENCY PLAN TO ENSURE AVAILABILITY OF CRITICAL ADP SYSTEMS. (p) |
| | • IDENTIFY THE CLASSIFICATION LEVEL OF ALL MAGNETIC MEDIA. (n) |
| | • PERFORM A RISK ASSESSMENT AT LEAST EVERY 3 YEARS. (p) |
| | • IDENTIFY ADP SECURITY TRAINING REQUIREMENTS AND DESIGNATE WHO WILL RECEIVE THE TRAINING. (p) |
| | • ASSIGN RESPONSIBILITY FOR CLASSIFIED ADP SYSTEMS. (p) |
| | • DEVELOP COMPUTER SECURITY MANUALS AND GUIDELINES FOR CLASSIFIED ADP SYSTEMS. (p) |
| | • REPORT ANY COMPUTER SECURITY INCIDENT. (p) |
| | • CONDUCT SECURITY SURVEYS OF ADP CENTERS. (m) |
| | • UTILIZE AUTHORIZED TECHNIQUES AND PROCEDURES FOR THE DESIGN, TESTING, AND EVALUATION OF CLASSIFIED ADP SYSTEMS. (p) |
| | • UTILIZE ONLY ACCREDITED OR APPROVED CLASSIFIED ADP SYSTEMS. (p) |
| | • MAINTAIN BACK-UP OF CRITICAL SOFTWARE AND DATA. (p) |
| | • PROVIDE CONFIGURATION MANAGEMENT CONTROLS FOR SOFTWARE, HARDWARE, AND SECURITY MECHANISMS. (p) |
| | • ASSIGN USERS A UNIQUE USER ID/PASSWORD. (p) |
| | • CHANGE USER PASSWORDS. (p) |
| | • ESTABLISH/UTILIZE AUDIT TRAILS. (p) |
| | • STORE AND LABEL CLASSIFIED MEDIA PROPERLY. (p) |
- N/A no classified data on computer system*

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

* Covers Hardware, Software, and Computer Security Related Procedures.

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF BASELINE
SECURITY REQUIREMENTS
FOR: PROCEDURES,
ADMINISTRATION, AND
SECURITY MANAGEMENT**

STEP 3

**WORKSHEET
W3.7**

System Name/Identification: Anonymous DOE Computer Center

SENSITIVE UNCLASSIFIED

- Y • ESTABLISH AND CONDUCT TRAINING AND AWARENESS FOR USE OF SENSITIVE DATA. (A,B,E,H)
- Y • ESTABLISH SECURITY INCIDENT/VIOLATION REPORTING SYSTEM. (E)
- Y • ESTABLISH AND IMPLEMENT PROCEDURES FOR PROVIDING DEVELOPED AND/OR MODIFIED SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE TO THE CENTRALIZED SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE ACTIVITY. (J)
- Y • ADVISE CENTRALIZED SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE ACTIVITY OF DIRECT EXCHANGE OF SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE WITH OTHER PROGRAMS OR SPECIFIC INFORMATION ANALYSIS CENTERS. (J)
- Y • COORDINATE WITH CENTRALIZED SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE FACILITY PRIOR TO DEVELOPING NEW SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE. (J)
- Y • IDENTIFY ALL SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE SENT TO THE CENTRALIZED FACILITY THAT HAS GENERAL UTILITY. (J)
- Y • ENSURE THAT THE APPROPRIATE INSTRUCTIONS FOR CONTROLLING DISSEMINATION OF SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE ARE INCLUDED IN ALL SCIENTIFIC AND TECHNICAL SOFTWARE PACKAGES PROVIDED TO THE CENTRALIZED FACILITY. (J)
- Y • ENSURE THAT PUBLIC DISSEMINATION OF COMPUTER SOFTWARE WHICH IS TRANSMITTED TO THE CENTRAL FACILITY WILL NEITHER VIOLATE THE U.S. EXPORT ADMINISTRATION REGULATIONS, THE INTERNATIONAL TRAFFIC IN ARMS REGULATIONS, THE NUCLEAR NONPROLIFERATION ACT, OR CONSTITUTE THE RELEASE OF SENSITIVE INFORMATION THAT WOULD OTHERWISE COMPROMISE NATIONAL SECURITY. (J)
- Y • ESTABLISH AND MAINTAIN A SYSTEM OF MANAGEMENT CONTROLS FOR ALL PROGRAMS AND ADMINISTRATIVE FUNCTIONS RELATED TO ADP EQUIPMENT ACQUISITION, COMPUTER FACILITY MANAGEMENT, EQUIPMENT UTILIZATION, SOFTWARE DEVELOPMENT, AND AUTOMATED MANAGEMENT INFORMATION SYSTEMS DEVELOPMENT, AS DIRECTED BY THE GAO AND DOE. (K)
- Y • DEVELOP MANAGEMENT CONTROL PLANS TO DESCRIBE THE SCHEDULE FOR ASSESSING VULNERABILITIES, IDENTIFYING AND IMPLEMENTING NEEDED IMPROVEMENTS, AND TESTING INTERNAL CONTROLS. (K)
- Y • EVALUATE THE EFFECTIVENESS OF INTERNAL CONTROLS ON A CONTINUING BASIS. (K)
- Y • ESTABLISH INTERNAL CONTROL PROGRAMS TO DETECT WASTE, LOSS, MISMANAGEMENT, UNAUTHORIZED USE, OR MISAPPROPRIATION. (K)
- Y • CONDUCT REVIEWS OF FINANCIAL MANAGEMENT SYSTEMS AS REQUIRED. (K)
- Y • DEVELOP A MANAGEMENT CONTROL PLAN AS APPROPRIATE. (K)
- Y • REPORT RESULTS OF INTERNAL CONTROL SYSTEM EVALUATIONS AS REQUIRED. (K)
- Y • ESTABLISH AND IMPLEMENT AN INTERNAL CONTROL ACTIVITY TRACKING PROGRAM AS APPROPRIATE. (K)

BOTH

- Y • ESTABLISH PROGRAM MANAGEMENT ORGANIZATION/POSITIONS FOR SENSITIVE/CLASSIFIED DATA AND PROGRAMS. (A,B,C,E)

CLASSIFIED

- ESTABLISH PROCEDURES FOR IDENTIFYING AND REPORTING VIOLATIONS OF LAW, LOSSES, AND INCIDENTS OF SECURITY INTEREST TO APPROPRIATE AUTHORITIES. (I)
- REPORT ANY SERIOUS SECURITY INCIDENTS TO THE IG. (m) N/A

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

(2) NOTE: Administrative Procedures for a specific security discipline (e.g., physical, computer, etc.) are listed under that discipline area.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
ENVIRONMENTAL
SECURITY/SAFETY**

STEP 3

**WORKSHEET
W3.8a**

System Name/Identification: Anonymous DOE Computer Center

BOTH

Y	• ESTABLISH/UTILIZE DESIGN REVIEW PROCESS FOR ALL NEW/MODIFIED BUILDINGS TO ASSURE FIRE DETECTION/PREVENTION ISSUES ARE ADDRESSED. (e)
Y	• SEGREGATE AND RESTRICT THE QUANTITY OF HAZARDOUS MATERIAL STORAGE. (e)
Y	• UTILIZE FLAME/SMOKE RESISTANT INTERIOR FINISH MATERIALS. (e)
Y	• SELECT FIRE PROTECTION SYSTEM BASED ON VALUE OF FACILITY AND CONTENTS. (e)
Y	• PROTECT STORAGE AREAS AND ROOMS AGAINST FIRES. (A, e)
Y	• SELECT FIRE PREVENTION MEASURES (AMOUNT, TYPE, ETC.) BASED ON IMPORTANCE OF PROGRAM (HOW VITAL IT IS) AND THE TIME ALLOWED FOR SHUT DOWN OF THAT PROGRAM. (e)
Y	• CONDUCT SELF-AUDITS AND INSPECTIONS USING FIRE PROTECTION EXPERTS. (e)
Y	• DEVELOP, MAINTAIN, TEST FIRE EMERGENCY PLAN. (e,f)
Y	• TRAIN PERSONNEL IN FIRE DETECTION/PREVENTION. (e)
Y	• INSTALL FIREWALLS, FIRE DOORS, DRAFT BARRIERS TO CONTAIN FIRE. (e)
Y	• IMPLEMENT SPECIAL FIRE CONTROL SYSTEM FOR HAZARDOUS MATERIALS. (e)
Y	• INSTALL AUTOMATIC FIRE DETECTION/REPORTING CAPABILITY. (e)
Y	• INSTALL AUTOMATIC SPRINKLER PROTECTION FOR ALL COMBUSTIBLE CONSTRUCTION AND COMPUTER ROOMS. (e,f)
Y	• UTILIZE METAL FURNISHINGS IN COMPUTER AREA. (f)
Y	• PROHIBIT SMOKING. (f)
Y	• PROHIBIT BULK STORAGE OF RECORDS, SUPPLIES, COMBUSTIBLE MATERIALS. (f)
Y	• UTILIZE NON-COMBUSTIBLE CABLE TRAYS AND FLAME RETARDENT INSULATION OR JACKETS FOR CABLES. (f)
Y	• INSTALL SEPARATE FIRE ALARM SYSTEM FOR COMPUTER ROOM. (e, f)
N	• LIMIT AMOUNT OF COMPUTER EQUIPMENT IN 1 ROOM TO \$1,000,000 VALUE AND HAVE 4 HOUR FIREWALLS WHEN VALUE DICTATES DIVISION OF AREA INTO SEPARATE ROOMS. (e)
Y	• DISALLOW AIR DUCTS THAT SERVE OTHER AREAS OR REQUIRE THAT THEY BE FIRE RESISTANT DUCTS. (e, f)
N	• AVOID BUNDLING CABLES IN LARGE GROUPS. (e, f)
Y	• REMOVE ALL ABANDONED CABLE FROM PREMISES. (e, f)
Y	• MINIMIZE STORAGE OF UNUSED CABLES UNDER FLOOR SPACES OR IN TRAYS. (e, f)
N	• STORE ALL COMPUTER PAPER SUPPLIES IN METAL CONTAINERS. (e, f)
Y	• PROMINENTLY LABEL MASTER CONTROL SWITCH FOR ALL EQUIPMENT AT EACH EXIT TO THE FACILITY. (e, f)

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS:
ENVIRONMENTAL
SECURITY/SAFETY**

STEP 3

WORKSHEET
W3.8b

System Name/Identification: Anonymous DOE Computer Center

BOTH (Continued)

Y	• INSTALL AUTOMATIC SPRINKLER AND DETECTION SYSTEMS IN STORAGE ROOMS/VULTS. (e, f)
Y	• INSTALL RAISED FLOORING. (e, f)
Y	• SITUATE COMPUTER FACILITIES IN NON-TRADITIONAL MOBILE BUILDING STRUCTURES A MINIMUM OF 50 FEET FROM NEAREST ADJOINING STRUCTURE AND CONSTRUCT WITH NON-COMBUSTIBLE MATERIALS. (f)
Y	• ASSIGN RESPONSIBILITY FOR IDENTIFYING FIRE AND PLANNING FACILITY'S FIRE PREVENTION AND DETECTION NEEDS. (e)

CLASSIFIED

	• PROHIBIT UNAUTHORIZED STORAGE OF SPECIAL NUCLEAR MATERIAL (m) <i>N/A</i>
--	--

Y: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

•: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**THREAT AND
VULNERABILITY
REVIEW**

**STEP 4
WORKSHEET
W4**

1. System Name/Identification: Anonymous DOE Computer Center

2. ASSET	(a) THREATS/VULNERABILITY(IES)	(b) PROBA- BILITY*	(c) PRIORITY FOR UPGRADE
a. Physical (Facility):			
b. Personnel:	<i>DOE employees not yet cleared may have access to unclassified but sensitive data because supervisors not advised of clearance status</i>	H	1
c. Information/Data, and Emissions:			
d. Communications:			
e. Computer (Hardware & Software):			
f. Procedures/ Administration/ Management:			
g. Environmental Security and Safety:	<i>Walls do not meet fire-rating standards causing rapid spread of fire.</i> <i>Paper supplies not stored in metal container creating a fire hazard.</i>	L L	3 2

* PROBABILITY KEY: HIGH (H) = THREAT IS VERY LIKELY TO OCCUR (ONE OR MORE TIMES A YEAR).
MEDIUM (M) = THREAT IS LIKELY TO OCCUR (ONCE EVERY 5 YEARS).
LOW (L) = THREAT IS UNLIKELY TO OCCUR (ONCE EVERY 10 YEARS OR LESS FREQUENTLY).

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT		THREATS TO AND VULNERABILITIES OF THE PHYSICAL FACILITY			STEP 4
					RESOURCE TABLE R4.18
PHYSICAL FACILITY		- IMPACT AREAS -			
		DAMAGE	DESTRUCTION	DISCLOSURE	DENIAL
NATURAL THREATS:					
*	STORMS	✓	✓	✓	✓
	EARTHQUAKES	✓	✓	✓	✓
	FIRE	✓	✓	✓	✓
	FLOOD	✓	✓	✓	✓
	HURRICANE	✓	✓	✓	✓
	TORNADO	✓	✓	✓	✓
INTENTIONAL HUMAN THREATS:					
*	TERRORIST INCIDENT	✓	✓	✓	✓
	BOMBING	✓	✓	✓	✓
	RIOT/CIVIL DISORDER	✓	✓	✓	✓
	SABOTAGE	✓	✓	✓	✓
	ARSON	✓	✓	✓	✓
	VANDALISM	✓	✓	✓	✓
	THEFT	✓	✓	✓	✓
	UNAUTHORIZED ACCESS	✓	✓	✓	✓
	MISAPPROPRIATION	✓	✓	✓	✓
	NEGLECT	✓	✓	✓	✓
	STRIKES	✓	✓	✓	✓
UNINTENTIONAL HUMAN THREATS:					
* *	ACCIDENTS	✓	✓	✓	✓
	OPERATIONAL/PROCEDURAL ERRORS	✓	✓	✓	✓
	HARDWARE FAILURE/MALFUNCTION	✓	✓	✓	✓
	NEGLECT	✓	✓	✓	✓
ENVIRONMENTAL THREATS:					
	HEATING/COOLING SYSTEM FAILURE	✓	✓		✓
	POWER FLUCTUATIONS/OUTAGE	✓	✓		✓
	TEMPERATURE/HUMIDITY FLUCTUATIONS	✓	✓		✓
	STRUCTURAL FAILURE	✓	✓	✓	✓

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**THREATS TO AND
VULNERABILITIES OF
PERSONNEL**

STEP 4

**RESOURCE
TABLE
R4.2a**

PERSONNEL

- IMPACT AREAS -

DAMAGE

DESTRUCTION

DISCLOSURE

DENIAL

NATURAL THREATS:

STORMS
EARTHQUAKES
FIRE
FLOOD
HURRICANE
POLLUTION
TORNADO
LIGHTNING

↓
↓
↓
↓
↓
↓
↓
↓

↓
↓
↓
↓
↓
↓
↓
↓

↓
↓
↓
↓
↓
↓
↓
↓

INTENTIONAL HUMAN THREATS:

TERRORIST INCIDENT
BOMBING
RIOT/CIVIL DISORDER
STRIKES
KIDNAPPING
ASSAULT
MURDER

↓
↓
↓
↓
↓
↓
↓

↓
↓
↓
↓
↓
↓
↓

↓
↓
↓
↓
↓
↓
↓

↓
↓
↓
↓
↓
↓
↓

UNINTENTIONAL HUMAN THREATS:

ACCIDENTS
OPERATIONAL/PROCEDURAL ERRORS
EMOTIONAL, MENTAL, HEALTH PROBLEMS

↓
↓
↓

↓
↓
↓

↓
↓
↓

↓
↓
↓

ENVIRONMENTAL THREATS:

HEATING/COOLING SYSTEM FAILURE
POWER OUTAGE
STRUCTURAL FAILURE

↓
↓

↓

↓
↓

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**THREATS TO AND
VULNERABILITIES OF
INFORMATION, DATA,
AND (DATA) EMISSIONS**

**STEP 4
RESOURCE
TABLE
R4.3a**

INFORMATION AND DATA

- IMPACT AREAS -

DAMAGE DESTRUCTION DISCLOSURE DENIAL

NATURAL THREATS:

STORMS		↓	↓	↓
EARTHQUAKES		↓	↓	↓
FIRE		↓	↓	↓
FLOOD		↓	↓	↓
HURRICANE		↓	↓	↓
POLLUTION	↓	↓	↓	↓
TORNADO	↓	↓	↓	↓
LIGHTNING	↓	↓	↓	↓

INTENTIONAL HUMAN THREATS:

TERRORIST INCIDENT	↓	↓	↓	↓
BOMBING	↓	↓	↓	↓
RIOT/CIVIL DISORDER	↓	↓	↓	↓
SABOTAGE	↓	↓	↓	↓
ARSON	↓	↓	↓	↓
VANDALISM	↓	↓	↓	↓
THEFT	↓	↓	↓	↓
UNAUTHORIZED ACCESS	↓	↓	↓	↓
MISAPPROPRIATION	↓	↓	↓	↓
WIRETAPPING/EAVESDROPPING	↓	↓	↓	↓
VIRUS	↓	↓	↓	↓
TRAP DOOR	↓	↓	↓	↓
TROJAN HORSE	↓	↓	↓	↓
MASQUERADE	↓	↓	↓	↓
ERASURE	↓	↓	↓	↓
EMISSION INTERCEPTION	↓	↓	↓	↓
STRIKES	↓	↓	↓	↓

UNINTENTIONAL HUMAN THREATS:

ACCIDENTS	↓	↓	↓	↓
OPERATIONAL/PROCEDURAL ERRORS	↓	↓	↓	↓
HARDWARE FAILURE/MALFUNCTION	↓	↓	↓	↓
SOFTWARE ERRORS	↓	↓	↓	↓
ERASURE	↓	↓	↓	↓
NEGLIGENCE	↓	↓	↓	↓
EMOTIONAL, MENTAL, HEALTH PROBLEMS	↓	↓	↓	↓

ENVIRONMENTAL THREATS:

HEATING/COOLING SYSTEM FAILURE	↓	↓	↓	↓
POWER FLUCTUATIONS/OUTAGE	↓	↓	↓	↓
TEMPERATURE/HUMIDITY FLUCTUATIONS	↓	↓	↓	↓
STRUCTURAL FAILURE	↓	↓	↓	↓

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**THREATS TO AND
VULNERABILITIES OF
COMMUNICATIONS**

STEP 4

**RESOURCE
TABLE
R4.4a**

COMMUNICATIONS

- IMPACT AREAS -

DAMAGE

DESTRUCTION

DISCLOSURE

DENIAL

NATURAL THREATS:

STORMS
EARTHQUAKES
FIRE
FLOOD
HURRICANE
TORNADO
LIGHTNING

↓
↓
↓
↓
↓
↓
↓

↓
↓
↓
↓
↓
↓
↓

↓
↓
↓
↓
↓
↓
↓

↓
↓
↓
↓
↓
↓
↓

INTENTIONAL HUMAN THREATS:

TERRORIST INCIDENT
BOMBING
RIOT/CIVIL DISORDER
SABOTAGE
ARSON
VANDALISM
THEFT
UNAUTHORIZED ACCESS
MISAPPROPRIATION
WIRETAPPING/EAVESDROPPING
NEGLECT
STRIKES

↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓

↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓

↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓

↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓
↓

UNINTENTIONAL HUMAN THREATS:

ACCIDENTS
OPERATIONAL/PROCEDURAL ERRORS
HARDWARE FAILURE/MALFUNCTION
NEGLECT

↓
↓
↓
↓

↓
↓
↓
↓

↓
↓
↓
↓

↓
↓
↓
↓

ENVIRONMENTAL THREATS:

HEATING/COOLING SYSTEM FAILURE
POWER FLUCTUATIONS/OUTAGE
TEMPERATURE/HUMIDITY FLUCTUATIONS
STRUCTURAL FAILURE

↓
↓
↓
↓

↓

↓

↓
↓
↓
↓

NOTE: Communications includes all communication capabilities and equipment: lines, networks, COMSEC security devices, protected distribution systems, phones, modems, etc.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**THREATS TO AND
VULNERABILITIES OF
COMPUTER
HARDWARE**

**STEP 4
RESOURCE
TABLE
R4.5a**

COMPUTER HARDWARE

- IMPACT AREAS -

DAMAGE

DESTRUCTION

DISCLOSURE

DENIAL

NATURAL THREATS:

STORMS
EARTHQUAKES
FIRE
FLOOD
HURRICANE
POLLUTION
TORNADO
LIGHTNING

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

INTENTIONAL HUMAN THREATS:

TERRORIST INCIDENT
BOMBING
RIOT/CIVIL DISORDER
SABOTAGE
ARSON
VANDALISM
THEFT
UNAUTHORIZED ACCESS
MISAPPROPRIATION
VIRUS
TRAP DOOR
TROJAN HORSE
NEGLECT
STRIKES

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

UNINTENTIONAL HUMAN THREATS:

ACCIDENTS
OPERATIONAL/PROCEDURAL ERRORS
HARDWARE FAILURE/MALFUNCTION
NEGLECT

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

ENVIRONMENTAL THREATS:

HEATING/COOLING SYSTEM FAILURE
POWER FLUCTUATIONS/OUTAGE
TEMPERATURE/HUMIDITY FLUCTUATIONS
STRUCTURAL FAILURE

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

↓

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**THREATS TO AND
VULNERABILITIES OF
ADP SYSTEM
PROCEDURES,
ADMINISTRATION AND
MANAGEMENT**

STEP 4
RESOURCE
TABLE
R4.6a

**ADP SYSTEM PROCEDURES,
ADMINISTRATION AND MANAGEMENT**

- IMPACT AREAS -

DAMAGE DESTRUCTION DISCLOSURE DENIAL

NATURAL THREATS:

STORMS	✓	✓	✓	✓
EARTHQUAKES	✓	✓	✓	✓
FIRE	✓	✓	✓	✓
FLOOD	✓	✓	✓	✓
HURRICANE	✓	✓	✓	✓
TORNADO	✓	✓	✓	✓

INTENTIONAL HUMAN THREATS:

TERRORIST INCIDENT	✓	✓	✓	✓
BOMBING	✓	✓	✓	✓
RIOT/CIVIL DISORDER	✓	✓	✓	✓
SABOTAGE	✓	✓	✓	✓
ARSON	✓	✓	✓	✓
VANDALISM	✓	✓	✓	✓
THEFT	✓	✓	✓	✓
UNAUTHORIZED ACCESS	✓	✓	✓	✓
NEGLECT	✓	✓	✓	✓

UNINTENTIONAL HUMAN THREATS:

ACCIDENTS	✓	✓	✓	✓
OPERATIONAL/PROCEDURAL ERRORS	✓	✓	✓	✓
NEGLECT	✓	✓	✓	✓
EMOTIONAL, MENTAL, HEALTH PROBLEMS	✓	✓	✓	✓

ENVIRONMENTAL THREATS:

POWER OUTAGE	✓		✓	✓
TEMPERATURE/HUMIDITY FLUCTUATIONS	✓	✓	✓	✓
STRUCTURAL FAILURE	✓		✓	✓

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**COUNTERMEASURES
IDENTIFICATION AND
RISK PROFILE ACCEPTANCE**

**STEP 5
WORKSHEET
W5**

1. System Name/Identification: Anonymous DOE Computer Center

2. SECURITY DISCIPLINE AREA	(a) ACCEPT CURRENT RISK PROFILE (YES OR NO)	(b) COUNTERMEASURES TO BE IMPLEMENTED	(c) APPROX. COST	(d) PRIORITY	(e) TARGET DATE
a. Physical Security:	Yes	None beyond those in place			
b. Personnel Security:	No	Establish procedures to notify supervisors of individual's clearance status	0	1	10/89
c. Information Security:	Yes	None beyond those in place			
d. Communications Security:	Yes	None beyond those in place			
e. Emissions Security (TEMPEST):	Yes	None beyond those in place			
f. Computer Security (Hardware & Software):	Yes	None beyond those in place			
g. Administrative/Procedural Security and Security Management	Yes	None beyond those in place			
h. Environmental Security and Safety:	No	Move equipment to new computer room Acquire metal containers for paper storage Reduce bundle size of cables	\$500 \$350 \$900	2 1 3	12/89 11/89 2/90

DOE/MA-365

DEPARTMENT OF ENERGY



VOLUME II

DOE RISK ASSESSMENT WORKSHEETS

-- A Structured Approach --

September, 1989

100

STEP 1
WORKSHEETS



**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SYSTEM COMPOSITION,
CONNECTIONS, AND
CONFIGURATION**

STEP 1
WORKSHEET
W1.1

1. System Name/Identification: _____
Organization/User: _____
Primary Use: _____
Location(s): _____
Date: _____

2. Connections:

Stand Alone System:

Network System:

LAN:

WAN:

: Open

: Closed

3. Configuration Diagram:

HWI

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**HARDWARE * INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.2**

1. System Name/identification: _____
 Organization/User: _____
 Primary Use: _____
 Location(s): _____
 Date: _____

2.	Hardware Inventory	Replacement Cost	
(a) Ref. No.	Description/Identification	(b) \$ Amount	OR (c) Rating (VH-VL)
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			
H -			

3. Total Replacement Cost \$ _____ or _____ Rating (VH, H, M, L, VL)

* NOTE: Hardware refers to the computer, peripherals, printer, and environmental and special support items.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SOFTWARE * INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.3**

1. System Name/Identification: _____
 Organization/User: _____
 Primary Use: _____
 Location(s): _____
 Date: _____

(a) Ref. No.	(b) Description/Identification	(c) Type Storage Media	(d) Does a Back-up Exist?	(e) Approx. Hours to Develop	Replacement Cost	
					(f) \$ Amount	(g) OR Rating (VH-VL)
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						
SW -						

3. Total Replacement Cost \$ _____ or _____ Rating (VH, H, M, L, VL)

* NOTE: Software includes all types of software, applications, and programs.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**DATA* INVENTORY
AND COST**

**STEP 1
WORKSHEET
W1.4**

1. System Name/Identification: _____
 Organization/User: _____
 Primary Use: _____
 Location(s): _____
 Date: _____

(a) Ref. No.	(b) Description/Identification	(c) Approx. Hrs. to Develop	(d) Does a Back-up Exist?	Replacement Cost	
				(e) \$ Amount	(f) OR Rating (VH-VL)
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					

3. Total Replacement Cost \$ _____ or _____ Rating (VH, H, M, L, VL)

* NOTE: Data refers to data sets used as input for processing or that result from processing.

STEP 2
WORKSHEETS



**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SYSTEM
CHARACTERISTICS
AND IMPORTANCE**

**STEP 2
WORKSHEET
W2.1**

(a) System *	(b) Number of Users (VL - VH)	(c) Frequency of Use (VL - VH)	(d) Impact if Unavailable (VL - VH)
System-1 Name/ID: <hr/> <hr/> <hr/>			
System-2 Name/ID: <hr/> <hr/> <hr/>			
System-3 Name/ID: <hr/> <hr/> <hr/>			
System-4 Name/ID: <hr/> <hr/> <hr/>			
System-5 Name/ID: <hr/> <hr/> <hr/>			

* NOTE: A system consists of the computer, peripherals, printer, environmental and other support items.



**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**SOFTWARE *
CHARACTERISTICS
AND IMPORTANCE**

**STEP 2
WORKSHEET
W2.2**

1. • System Name/Identification: _____
 • Organization/Owner: _____
 • Location(s): _____
 • Date: _____

NOTE: Use reference numbers from Worksheet W1.3 to avoid retyping all entries.

2. Ref. No.	a) Software Sensitivity or Classification			b) Frequency of Use	c) Impact If Unavailable
	1) Unclassified?	2) Sensitive Unclassified? (Type)	3) Classified? (Note Level and Mode of Operation)		
SW -					
SW -					
SW -					
SW -					
SW -					
SW -					
SW -					
SW -					
SW -					
SW -					
SW -					
SW -					
SW -					
SW -					
SW -					
SW -					
3. Approx. ** %	_____ %	_____ %	_____ %		

* Software includes all types of software, applications, and programs.
 ** Total of columns 1, 2, and 3 should = 100% (reflecting all software (applications, programs) used).

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**DATA *
CHARACTERISTICS
AND IMPORTANCE**

**STEP 2
WORKSHEET
W2.3**

1. • System Name/identification: _____
 • Organization/User: _____
 • Location(s): _____
 • Date: _____

NOTE: Use reference numbers from Worksheet W1.4 to avoid restating all entries.

2. Ref. No.	(e) Data Sensitivity or Classification			b) Frequency of Use	c) Impact If Unavailable
	1) Unclassified?	2) Sensitive Unclassified? (Note Type)	3) Classified? (Note Level)		
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
D -					
3. Approx. %	_____ %	_____ %	_____ %		

* Data refers to specific data sets used as input for processing or that result from processing.

** Total of columns 1, 2, and 3 should = 100% of all data used.





STEP 3
WORKSHEETS



System Name/Identification: _____

SENSITIVE UNCLASSIFIED

- | | |
|--|---|
| | • STORE INFORMATION/DATA IN UNLOCKED FILES, DESKS WITHIN CONTROLLED/GUARDED AREA. (B) |
| | • STORE INFORMATION/DATA IN LOCKED REPOSITORY IN UNCONTROLLED/GUARDED AREA. (B) |

BOTH

- | | |
|--|---|
| | • DEFINE PHYSICAL SECURITY REQUIREMENTS FOR ADP OPERATIONS AT ONSET OF PROGRAM. (D) |
| | • UTILIZE A PERSONNEL IDENTIFICATION SYSTEM FOR FACILITY WITH 30+ INDIVIDUALS. (q, r, u) |
| | • RECOVER BADGES OF TERMINATING EMPLOYEES AND DEPARTING VISITORS. (u) |
| | • REPLACE BADGES AND PASSES AS APPROPRIATE. (u) |
| | • RETAIN RECORD OF LOST BADGES, PASSES, CREDENTIALS, AND SHIELDS. (u) |
| | • DESIGN ELECTRONIC ALARMS TO MEET SITE-SPECIFIC PROTECTION NEEDS AND REQUIREMENTS IN DOE 5632.5. (q) |
| | • USE A RECEPTIONIST OR EMPLOYEE WITH ASSIGNED RESPONSIBILITY TO CONTROL ACCESS DURING WORKING HOURS. (r) |
| | • MAINTAIN A VISITORS LOG. (r) |
| | • POST TRESPASSING SIGNS AROUND PERIMETER AND ENTRANCES. (r) |
| | • INSPECT AND SEARCH VEHICLES AND HAND CARRIED ITEMS RANDOMLY. (r) |
| | • POST CONTRABAND/PROHIBITED ITEMS SIGN AT ALL ENTRANCES. (r) |
| | • IMPEDE ACCESS WITH BARRIERS (I.E., WALLS, FENCES, ETC.). (r) |
| | • LOCK AREA, BUILDING, ADP CENTER, ETC. WHEN UNOCCUPIED. (r) |
| | • UTILIZE LOCKS THAT ARE GSA/GOVERNMENT APPROVED. (r) |
| | • CONTROL AND ACCOUNT FOR ALL KEYS AND COMBINATIONS. (r) |
| | • CHANGE LOCKS AND COMBINATIONS WHEN LOST/COMPROMISED. (r) |
| | • PROVIDE INTRUSION DETECTION SYSTEM AS APPROPRIATE. (r) |
| | • TEST AND MAINTAIN ALARM/SECURITY SYSTEMS AND COMPONENTS IN OPERABLE CONDITION. (r) |
| | • ESTABLISH EMERGENCY PLANS. (r) |
| | • DESIGN ELECTRONIC ALARMS TO MEET SITE-SPECIFIC PROTECTION NEEDS AND REQUIREMENTS WITH DOE ALARM REQUIREMENTS. (q) |

KEY: YES = Y	NO = N	NOT APPLICABLE = N/A	PARTIALLY = P
--------------	--------	----------------------	---------------

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.



**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
PHYSICAL SECURITY**

**STEP 3
WORKSHEET
W3.1b**

System Name/Identification: _____

CLASSIFIED

- DETECT AND DETER UNAUTHORIZED ACCESS TO ADP CENTERS. (q)
- ESTABLISH SECURITY AREAS AS REQUIRED BY DOE BASED ON MISSION AND SIZE. (a)
- SAFEGUARD STOCK OF UNUSED BADGES, PASSES, CREDENTIALS, AND SHIELDS. (u)
- IDENTIFY SECURITY IMPORTANCE RATINGS OF SECURE FACILITIES. (m)
- CONTROL AND LIMIT ACCESS TO PERSONNEL WHO ARE CLEARED FOR ACCESS TO THE HIGHEST CLASSIFICATION LEVEL OF INFORMATION. (p, q)
- ESTABLISH A TSCM PROGRAM FOR FACILITIES THAT HOUSE CLASSIFIED ADP SYSTEMS. (o)
- NOTIFY RESPONSIBLE ORGANIZATION OF PHYSICAL SECURITY DEFICIENCIES. (m)
- CONDUCT INITIAL AND PERIODIC SECURITY SURVEYS TO ENSURE DOE SECURITY POLICIES AND PROCEDURES ARE IMPLEMENTED. (m)

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

System Name/Identification: _____

SENSITIVE UNCLASSIFIED

- | | |
|--|---|
| | • LIMIT PERSONNEL ACCESS TO SENSITIVE UNCLASSIFIED MATERIALS VIA DISSEMINATION AND ACCESS CONTROLS. (B,E,F,H) |
| | • SCREEN ALL PERSONNEL INVOLVED WITH SENSITIVE DATA. (E) |
| | • REQUIRE PROOF OF IDENTITY TO RECEIPT FOR INFORMATION. (H) |

CLASSIFIED

- | | |
|--|---|
| | • CONTROL AND LIMIT ACCESS TO CLASSIFIED INFORMATION TO AUTHORIZED PERSONNEL ONLY. (n, p) |
| | • LIMIT PERSONNEL ACCESS TO WEAPONS DATA MATERIALS VIA DISSEMINATION AND ACCESS CONTROLS. (v) |
| | • CONTROL ACCESS TO FOREIGN INTELLIGENCE INFORMATION. (x) |
| | • ENSURE PERSONNEL ARE COGNIZANT OF THEIR RESPONSIBILITIES TO SAFEGUARD AND CONTROL CLASSIFIED DOCUMENTS. (n) |
| | • OBTAIN NECESSARY VISITOR ACCESS AUTHORIZATIONS PRIOR TO PERMITTING ACCESS TO FACILITIES CONTAINING NAVAL NUCLEAR PROPULSION INFORMATION (NNPI). (h) |
| | • ENSURE THAT ALL INDIVIDUALS REQUIRING ACCESS TO CLASSIFIED MATERIAL ARE APPROPRIATELY CLEARED. (g) |

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
INFORMATION SECURITY**

STEP 3

**WORKSHEET
W3.3**

System Name/Identification: _____

SENSITIVE UNCLASSIFIED

- MAINTAIN CURRENT INVENTORY OF STORED INFORMATION. (A)
- USE COVER SHEETS AND SPECIAL MARKINGS FOR UCNI. (B)
- STORE UCNI MATERIALS IN LOCKED REPOSITORY. (B)
- STORE UCNI MATERIALS IN UNLOCKED FILES AND DESKS IF WITHIN CONTROLLED/GUARDED AREA. (B)
- SHRED OR BURN MEDIA TO BE DESTROYED. (B)
- PROTECT COMPUTER SECURITY PROGRAM INFORMATION. (B,E)
- REVIEW VITAL RECORDS ANNUALLY. (A)
- APPROPRIATELY MARK ON THE COVER AND TITLE PAGE OF ALL SOFTWARE DOCUMENTATION FOR SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE WHICH MAY BE DISSEMINATED TO OTHERS. (J)
- UTILIZE OPSEC TECHNIQUES OR MEASURES TO PROTECT CLASSIFIED OR SENSITIVE/UNCLASSIFIED INFORMATION. (K)
- PREPARE AN OPSEC THREAT STATEMENT AND DEVELOP A CRITICAL AND SENSITIVE INFORMATION LIST AND SUPPORTING ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION. (K)
- DEVELOP PROCEDURES FOR PROPERLY REPORTING, HANDLING, SAFEGUARDING, AND DISPOSING OF DOE SCIENTIFIC AND TECHNICAL INFORMATION. (I)
- PROHIBIT DUPLICATION OF SOFTWARE, DATA FOR PERSONAL USE OR ON HOME COMPUTERS. (L)

BOTH

- IDENTIFY ALL SENSITIVE DATA, INFORMATION, MATERIALS. (A,C,E,F)
- DEFINE INFORMATION SECURITY NEEDS AT ONSET OF ALL PROGRAMS. (D)
- REVIEW PROGRAMS AND DATA FOR COMPLIANCE WITH REQUIREMENTS FOR HANDLING AND CONTROL OF SENSITIVE DATA. (A,C,E,H)
- MARK SENSITIVE UNCLASSIFIED AND CLASSIFIED MATERIAL AND EQUIPMENT WITH NECESSARY MARKINGS EITHER BY STAMPING, TAGS, LABELS, OR OTHER SUITABLE MEANS. (q)
- STORE SENSITIVE OR CLASSIFIED MATTER IN SECURITY CONTAINERS. (q)

CLASSIFIED

- MAINTAIN ACCOUNTABILITY SYSTEM, AS APPROPRIATE, TO ACCOUNT FOR AND DETERMINE WHEN CLASSIFIED MATTER IS LOST OR UNACCOUNTED FOR. (a)
- MARK CLASSIFIED MATERIAL, MEDIA, AND OTHER EQUIPMENT WITH CLASSIFICATION AND OTHER NECESSARY MARKINGS, EITHER BY STAMPING, TAGS, LABELS, OR OTHER SUITABLE MEANS. (q)
- STORE CLASSIFIED MATTER IN APPROVED SECURITY CONTAINERS. (q)
- CONDUCT ANNUAL REVIEW OF TOP SECRET DOCUMENTS. (n)
- AFFIX SPECIAL HANDLING MARKINGS TO NNPI AS APPROPRIATE. (h)

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT	REVIEW OF BASELINE SECURITY REQUIREMENTS FOR: COMMUNICATIONS SECURITY (COMSEC)	STEP 3
		WORKSHEET W3.4
System Name/Identification: _____		
SENSITIVE UNCLASSIFIED		
	AS APPROPRIATE:	
	<ul style="list-style-type: none"> • USE OF PRIVACY DEVICES TO PROTECT UNCLASSIFIED INFORMATION. (c) 	
	<ul style="list-style-type: none"> • USE OF DES TO PROTECT UNCLASSIFIED, SENSITIVE INFORMATION. (c) 	
BOTH		
	<ul style="list-style-type: none"> • PROCURE/USE CRYPTO GEAR FOR UNCLASSIFIED SENSITIVE DISCUSSIONS/TRANSMISSIONS, IF DEEMED NECESSARY. (c) 	
	<ul style="list-style-type: none"> • DESIGN AND INSTALL PDS, AS APPROPRIATE. (d) 	
	<ul style="list-style-type: none"> • SECURE CLASSIFIED AND UNCLASSIFIED SENSITIVE SYSTEMS TO PREVENT COMPROMISE OR EXPLOITATION. (c) 	
CLASSIFIED		
	<ul style="list-style-type: none"> • CONDUCT SECURITY SURVEYS OF SECURE COMMUNICATIONS CENTERS. (m) 	
	<ul style="list-style-type: none"> • PROCURE/USE NSA APPROVED CRYPTOGRAPHIC DEVICES. (p) 	
	<ul style="list-style-type: none"> • ENSURE CLASSIFIED INFORMATION IS NOT DISCUSSED OR TRANSMITTED OVER UNENCRYPTED OR NONSECURE TELEPHONE SYSTEMS. (n) 	
	<ul style="list-style-type: none"> • PROCURE/USE CRYPTO GEAR FOR CLASSIFIED DISCUSSIONS/TRANSMISSIONS. (c) 	

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P
--

- (1) NOTE: Additional PDS Guidance is provided in the DOE PDS Procedural Guide (u) (Confidential).
- (2) NOTE: Additional COMSEC guidance regarding the role and responsibilities of the CRYPTO custodian are provided in the DOE COMSEC Procedural Guide (u) (Confidential).
- (3) NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
EMISSIONS SECURITY
(TEMPEST)**

STEP 3

**WORKSHEET
W3.5**

System Name/Identification: _____

BOTH SENSITIVE UNCLASSIFIED/CLASSIFIED

AS APPROPRIATE:

- APPOINT TEMPEST COORDINATOR. (b)
- PERFORM TEMPEST SURVEYS. (b)
- ZONE TEST EVERY 3 YEARS. (b)
- MAINTAIN TEMPEST FILE FOR EACH FACILITY. (b)
- COMPLY WITH EMISSIONS SECURITY REQUIREMENTS. (b)

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

(1) NOTE: Additional TEMPEST guidance is provided in the DOE TEMPEST Procedural Guide (u) (Confidential). As of May 1989, this guide was undergoing a major update/revision.

(2) NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT

REVIEW OF BASELINE SECURITY REQUIREMENTS FOR: COMPUTER SECURITY*

STEP 3

WORKSHEET
W3.6a

System Name/Identification: _____

SENSITIVE UNCLASSIFIED

- DEFINE OPERATING AND APPLICATION SOFTWARE SECURITY NEEDS AT ONSET OF PROGRAM. (D,E,H)
- MAINTAIN ACCESS LOG(S) TO DETECT UNAUTHORIZED ACCESS ATTEMPTS. (E)
- RANDOMLY REVIEW FILE CONTENTS. (E)
- ESTABLISH CONFIGURATION MANAGEMENT CONTROLS TO TRACK HARDWARE AND SOFTWARE SECURITY UPGRADES BASED ON RESULTS OF RISK ASSESSMENT. (E)
- DETERMINE IMPORTANCE OF APPLICATION TO MISSION. (E)
- DEVELOP COMPUTER PROTECTION PLAN. (E)
- ESTABLISH AND IMPLEMENT COMPUTER SECURITY CONTROL PROCEDURES TO PROTECT HARDWARE, SOFTWARE, AND DATA AGAINST THEFT, LOSS, UNAUTHORIZED MANIPULATION, FRAUDULENT ACTIVITIES AND NATURAL DISASTERS. (K)
- ADVISE APPROPRIATE AUTHORITIES OF ANY SENSITIVE/UNCLASSIFIED COMPUTER SECURITY VULNERABILITY DETECTED IN THE COURSE OF AN OPSEC VULNERABILITY ASSESSMENT. (K)
- ESTABLISH AND IMPLEMENT COMPUTER OPERATION CONTROL PROCEDURES TO ENSURE ACCURACY AND COMPLETENESS OF THE INFORMATION MAINTAINED AND PROCESSED. (K)
- ESTABLISH, DOCUMENT, AND ENFORCE PROCEDURES FOR TESTING AND IMPLEMENTING SOFTWARE CHANGES. (K)
- ESTABLISH AND IMPLEMENT HARDWARE CONTROLS FOR ALL HARDWARE PROCUREMENT ACTIONS. (K)
- ESTABLISH AND ENFORCE CONTROL PROCEDURES FOR DISTRIBUTED PROCESSING AND NETWORK OPERATIONS. (K)
- REQUIRE THAT SYSTEM DESIGN, DEVELOPMENT, AND MODIFICATION CONTROL PROCEDURES PROVIDE ADEQUATE SEPARATION OF DUTIES AND ASSURES USER, MANAGEMENT, AND INTERNAL AUDITOR PARTICIPATION. (K)
- ESTABLISH CONTROL MECHANISMS TO ENSURE THAT DATA REACHES THE COMPUTER APPLICATION WITHOUT LOSS, UNAUTHORIZED ADDITION OR MODIFICATION, OR OTHER ERROR. (K)
- ESTABLISH AND ENFORCE PROCEDURES FOR CONVERTING AND ENTERING DATA THROUGH TERMINALS AND DETAIL THE PROCESS FOR IDENTIFYING, CORRECTING, AND REPROCESSING DATA REJECTED BY THE APPLICATION. (K)
- DEVELOP, DOCUMENT AND IMPLEMENT CONTROL PROCEDURES FOR PROCESSING DATA AND SCHEDULING DATA PROCESSING. (K)
- DEVELOP, DOCUMENT, AND IMPLEMENT OUTPUT CONTROL PROCEDURES. (K)
- DEVELOP AND IMPLEMENT EFFECTIVE CONTROLS FOR THE ACQUISITION, OPERATION AND SECURITY OF MICROCOMPUTERS. (K)
- REQUIRE WRITTEN AUTHORIZATION TO USE COMPUTER EQUIPMENT FOR OFF-SITE WORK. (L)

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

* Covers Hardware, Software, and Computer Security Related Procedures.

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
COMPUTER SECURITY ***

STEP 3

**WORKSHEET
W3.6b**

System Name/Identification: _____

BOTH

- PROVIDE CONFIGURATION MANAGEMENT CONTROLS. (C, E)
- REVIEW/APPROVE AND CERTIFY DESIGN OF NEW OR CHANGED HARDWARE/SOFTWARE. (C,D,E,H)
- DEFINE, EVALUATE, AND REEVALUATE SECURITY REQUIREMENTS THROUGHOUT SYSTEM LIFE-CYCLE. (C,D,E,H)
- AUDIT SYSTEM, (C,E,p)
- DEVELOP AND TEST CONTINGENCY PLAN, INCLUDING BACK-UP AND RECOVERY FEATURES. (A,C,p)
- TEST HARDWARE AND SOFTWARE PROTECTIVE FEATURES. (E, p)

CLASSIFIED

- PREPARE ADP SECURITY PLAN. (p)
- DEVELOP, IMPLEMENT, MAINTAIN, AND DOCUMENT ALL ADP SECURITY MEASURES. (p)
- CLEAR AND SANITIZE ADP RESOURCES FOR CLASSIFIED PROCESSING. (p)
- DEVELOP A CONTINGENCY PLAN TO ENSURE AVAILABILITY OF CRITICAL ADP SYSTEMS. (p)
- IDENTIFY THE CLASSIFICATION LEVEL OF ALL MAGNETIC MEDIA. (n)
- PERFORM A RISK ASSESSMENT AT LEAST EVERY 3 YEARS. (p)
- IDENTIFY ADP SECURITY TRAINING REQUIREMENTS AND DESIGNATE WHO WILL RECEIVE THE TRAINING. (p)
- ASSIGN RESPONSIBILITY FOR CLASSIFIED ADP SYSTEMS. (p)
- DEVELOP COMPUTER SECURITY MANUALS AND GUIDELINES FOR CLASSIFIED ADP SYSTEMS. (p)
- REPORT ANY COMPUTER SECURITY INCIDENT. (p)
- CONDUCT SECURITY SURVEYS OF ADP CENTERS. (m)
- UTILIZE AUTHORIZED TECHNIQUES AND PROCEDURES FOR THE DESIGN, TESTING, AND EVALUATION OF CLASSIFIED ADP SYSTEMS. (p)
- UTILIZE ONLY ACCREDITED OR APPROVED CLASSIFIED ADP SYSTEMS. (p)
- MAINTAIN BACK-UP OF CRITICAL SOFTWARE AND DATA. (p)
- PROVIDE CONFIGURATION MANAGEMENT CONTROLS FOR SOFTWARE, HARDWARE, AND SECURITY MECHANISMS. (p)
- ASSIGN USERS A UNIQUE USER ID/PASSWORD. (p)
- CHANGE USER PASSWORDS. (p)
- ESTABLISH/UTILIZE AUDIT TRAILS. (p)
- STORE AND LABEL CLASSIFIED MEDIA PROPERLY. (p)

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

* Covers Hardware, Software, and Computer Security Related Procedures.

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF BASELINE
SECURITY REQUIREMENTS
FOR: PROCEDURES,
ADMINISTRATION, AND
SECURITY MANAGEMENT**

STEP 3

**WORKSHEET
W3.7**

System Name/Identification: _____

SENSITIVE UNCLASSIFIED

- ESTABLISH AND CONDUCT TRAINING AND AWARENESS FOR USE OF SENSITIVE DATA. (A,B,E,H)
- ESTABLISH SECURITY INCIDENT/VIOLATION REPORTING SYSTEM. (E)
- ESTABLISH AND IMPLEMENT PROCEDURES FOR PROVIDING DEVELOPED AND/OR MODIFIED SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE TO THE CENTRALIZED SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE ACTIVITY. (J)
- ADVISE CENTRALIZED SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE ACTIVITY OF DIRECT EXCHANGE OF SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE WITH OTHER PROGRAMS OR SPECIFIC INFORMATION ANALYSIS CENTERS. (J)
- COORDINATE WITH CENTRALIZED SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE FACILITY PRIOR TO DEVELOPING NEW SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE. (J)
- IDENTIFY ALL SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE SENT TO THE CENTRALIZED FACILITY THAT HAS GENERAL UTILITY. (J)
- ENSURE THAT THE APPROPRIATE INSTRUCTIONS FOR CONTROLLING DISSEMINATION OF SCIENTIFIC AND TECHNICAL COMPUTER SOFTWARE ARE INCLUDED IN ALL SCIENTIFIC AND TECHNICAL SOFTWARE PACKAGES PROVIDED TO THE CENTRALIZED FACILITY. (J)
- ENSURE THAT PUBLIC DISSEMINATION OF COMPUTER SOFTWARE WHICH IS TRANSMITTED TO THE CENTRAL FACILITY WILL NEITHER VIOLATE THE U.S. EXPORT ADMINISTRATION REGULATIONS, THE INTERNATIONAL TRAFFIC IN ARMS REGULATIONS, THE NUCLEAR NONPROLIFERATION ACT, OR CONSTITUTE THE RELEASE OF SENSITIVE INFORMATION THAT WOULD OTHERWISE COMPROMISE NATIONAL SECURITY. (J)
- ESTABLISH AND MAINTAIN A SYSTEM OF MANAGEMENT CONTROLS FOR ALL PROGRAMS AND ADMINISTRATIVE FUNCTIONS RELATED TO ADP EQUIPMENT ACQUISITION, COMPUTER FACILITY MANAGEMENT, EQUIPMENT UTILIZATION, SOFTWARE DEVELOPMENT, AND AUTOMATED MANAGEMENT INFORMATION SYSTEMS DEVELOPMENT, AS DIRECTED BY THE GAO AND DOE. (K)
- DEVELOP MANAGEMENT CONTROL PLANS TO DESCRIBE THE SCHEDULE FOR ASSESSING VULNERABILITIES, IDENTIFYING AND IMPLEMENTING NEEDED IMPROVEMENTS, AND TESTING INTERNAL CONTROLS. (K)
- EVALUATE THE EFFECTIVENESS OF INTERNAL CONTROLS ON A CONTINUING BASIS. (K)
- ESTABLISH INTERNAL CONTROL PROGRAMS TO DETECT WASTE, LOSS, MISMANAGEMENT, UNAUTHORIZED USE, OR MISAPPROPRIATION. (K)
- CONDUCT REVIEWS OF FINANCIAL MANAGEMENT SYSTEMS AS REQUIRED. (K)
- DEVELOP A MANAGEMENT CONTROL PLAN AS APPROPRIATE. (K)
- REPORT RESULTS OF INTERNAL CONTROL SYSTEM EVALUATIONS AS REQUIRED. (K)
- ESTABLISH AND IMPLEMENT AN INTERNAL CONTROL ACTIVITY TRACKING PROGRAM AS APPROPRIATE. (K)

BOTH

- ESTABLISH PROGRAM MANAGEMENT ORGANIZATION/POSITIONS FOR SENSITIVE/CLASSIFIED DATA AND PROGRAMS. (A,B,C,E)

CLASSIFIED

- ESTABLISH PROCEDURES FOR IDENTIFYING AND REPORTING VIOLATIONS OF LAW, LOSSES, AND INCIDENTS OF SECURITY INTEREST TO APPROPRIATE AUTHORITIES. (I)
- REPORT ANY SERIOUS SECURITY INCIDENTS TO THE IG. (m)

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

1) NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

(2) NOTE: Administrative Procedures for a specific security discipline (e.g., physical, computer, etc.) are listed under that discipline area.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS FOR:
ENVIRONMENTAL
SECURITY/SAFETY**

STEP 3

**WORKSHEET
W3.8a**

System Name/Identification: _____

BOTH

- ESTABLISH/UTILIZE DESIGN REVIEW PROCESS FOR ALL NEW/MODIFIED BUILDINGS TO ASSURE FIRE DETECTION/PREVENTION ISSUES ARE ADDRESSED. (e)
- SEGREGATE AND RESTRICT THE QUANTITY OF HAZARDOUS MATERIAL STORAGE. (e)
- UTILIZE FLAME/SMOKE RESISTANT INTERIOR FINISH MATERIALS. (e)
- SELECT FIRE PROTECTION SYSTEM BASED ON VALUE OF FACILITY AND CONTENTS. (e)
- PROTECT STORAGE AREAS AND ROOMS AGAINST FIRES. (A, e)
- SELECT FIRE PREVENTION MEASURES (AMOUNT, TYPE, ETC.) BASED ON IMPORTANCE OF PROGRAM (HOW VITAL IT IS) AND THE TIME ALLOWED FOR SHUT DOWN OF THAT PROGRAM. (e)
- CONDUCT SELF-AUDITS AND INSPECTIONS USING FIRE PROTECTION EXPERTS. (e)
- DEVELOP, MAINTAIN, TEST FIRE EMERGENCY PLAN. (e,f)
- TRAIN PERSONNEL IN FIRE DETECTION/PREVENTION. (e)
- INSTALL FIREWALLS, FIRE DOORS, DRAFT BARRIERS TO CONTAIN FIRE. (e)
- IMPLEMENT SPECIAL FIRE CONTROL SYSTEM FOR HAZARDOUS MATERIALS. (e)
- INSTALL AUTOMATIC FIRE DETECTION/REPORTING CAPABILITY. (e)
- INSTALL AUTOMATIC SPRINKLER PROTECTION FOR ALL COMBUSTIBLE CONSTRUCTION AND COMPUTER ROOMS. (e,f)
- UTILIZE METAL FURNISHINGS IN COMPUTER AREA. (f)
- PROHIBIT SMOKING. (f)
- PROHIBIT BULK STORAGE OF RECORDS, SUPPLIES, COMBUSTIBLE MATERIALS. (f)
- UTILIZE NON-COMBUSTIBLE CABLE TRAYS AND FLAME RETARDENT INSULATION OR JACKETS FOR CABLES. (f)
- INSTALL SEPARATE FIRE ALARM SYSTEM FOR COMPUTER ROOM. (e, f)
- LIMIT AMOUNT OF COMPUTER EQUIPMENT IN 1 ROOM TO \$1,000,000 VALUE AND HAVE 4 HOUR FIREWALLS WHEN VALUE DICTATES DIVISION OF AREA INTO SEPARATE ROOMS. (e)
- DISALLOW AIR DUCTS THAT SERVE OTHER AREAS OR REQUIRE THAT THEY BE FIRE RESISTANT DUCTS. (e, f)
- AVOID BUNDLING CABLES IN LARGE GROUPS. (e, f)
- REMOVE ALL ABANDONED CABLE FROM PREMISES. (e, f)
- MINIMIZE STORAGE OF UNUSED CABLES UNDER FLOOR SPACES OR IN TRAYS. (e, f)
- STORE ALL COMPUTER PAPER SUPPLIES IN METAL CONTAINERS. (e, f)
- PROMINENTLY LABEL MASTER CONTROL SWITCH FOR ALL EQUIPMENT AT EACH EXIT TO THE FACILITY. (e, f)

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.

**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**REVIEW OF
BASELINE SECURITY
REQUIREMENTS:
ENVIRONMENTAL
SECURITY/SAFETY**

STEP 3

**WORKSHEET
W3.8b**

System Name/Identification: _____

BOTH (Continued)

- INSTALL AUTOMATIC SPRINKLER AND DETECTION SYSTEMS IN STORAGE ROOMS/VAULTS. (e, f)
- INSTALL RAISED FLOORING. (e, f)
- SITUATE COMPUTER FACILITIES IN NON-TRADITIONAL MOBILE BUILDING STRUCTURES A MINIMUM OF 50 FEET FROM NEAREST ADJOINING STRUCTURE AND CONSTRUCT WITH NON-COMBUSTIBLE MATERIALS. (f)
- ASSIGN RESPONSIBILITY FOR IDENTIFYING FIRE AND PLANNING FACILITY'S FIRE PREVENTION AND DETECTION NEEDS. (e)

CLASSIFIED

- PROHIBIT UNAUTHORIZED STORAGE OF SPECIAL NUCLEAR MATERIAL (m)

KEY: YES = Y NO = N NOT APPLICABLE = N/A PARTIALLY = P

NOTE: A letter in parenthesis follows each title or individual entry. Each letter refers to a specific DOE order. To identify the specific document from which a requirement is taken, refer to the Master List, Resource Table R3.



STEP 4
WORKSHEETS



DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT	THREATS TO AND VULNERABILITIES OF THE PHYSICAL FACILITY			STEP 4
	WORKSHEET W4.1			
PHYSICAL FACILITY *	-- IMPACT AREAS --			
	DAMAGE	DESTRUCTION	DISCLOSURE	DENIAL
NATURAL THREATS:				
STORMS	√	√	√	√
EARTHQUAKES	√	√	√	√
FIRE	√	√	√	√
FLOOD	√	√	√	√
HURRICANE	√	√	√	√
TORNADO	√	√	√	√
INTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER*				
TERRORIST INCIDENT	√	√	√	√
BOMBING	√	√	√	√
RIOT/CIVIL DISORDER	√	√	√	√
SABOTAGE	√	√	√	√
ARSON	√	√	√	√
VANDALISM	√	√	√	√
THEFT	√	√	√	√
UNAUTHORIZED ACCESS	√	√	√	√
MISAPPROPRIATION	√	√	√	√
NEGLECT	√	√	√	√
STRIKES				√
UNINTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
ACCIDENTS	√	√	√	√
OPERATIONAL/PROCEDURAL ERRORS	√	√	√	√
HARDWARE FAILURE/MALFUNCTION	√	√	√	√
NEGLECT	√	√	√	√
ENVIRONMENTAL THREATS:				
HEATING/COOLING SYSTEM FAILURE	√	√		√
POWER FLUCTUATIONS/OUTAGE				√
TEMPERATURE/HUMIDITY FLUCTUATIONS	√	√		√
STRUCTURAL FAILURE	√	√	√	√

* PHYSICAL FACILITY INCLUDES THE BUILDING, COMPUTER ROOM, SUPPORTING UTILITIES, NON-ADP EQUIPMENT, AND SUPPLIES.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT	THREATS TO AND VULNERABILITIES OF PERSONNEL			STEP 4
				WORKSHEET W4.2
PERSONNEL *	- IMPACT AREAS -			
	DAMAGE	DESTRUCTION	DISCLOSURE	DENIAL
NATURAL THREATS:				
STORMS	√	√		√
EARTHQUAKES	√	√		√
FIRE	√	√		√
FLOOD	√	√		√
HURRICANE	√	√		√
POLLUTION	√	√		√
TORNADO	√	√		√
LIGHTNING	√	√		√
INTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
TERRORIST INCIDENT	√	√	√	√
BOMBING	√	√		√
RIOT/CIVIL DISORDER	√	√		√
STRIKES				√
KIDNAPPING	√	√	√	√
ASSAULT	√	√	√	√
MURDER		√		√
UNINTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
ACCIDENTS	√	√	√	√
OPERATIONAL/PROCEDURAL ERRORS	√	√	√	√
EMOTIONAL, MENTAL, HEALTH PROBLEMS	√	√	√	√
ENVIRONMENTAL THREATS:				
HEATING/COOLING SYSTEM FAILURE	√			√
POWER OUTAGE				√
STRUCTURAL FAILURE	√	√		√

* PERSONNEL INCLUDES THE COMPUTER OPERATOR(S), SYSTEM MANAGER, COMPUTER SECURITY OFFICIAL, DATA BASE ADMINISTRATOR, ETC.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT	THREATS TO AND VULNERABILITIES OF INFORMATION, DATA, AND EMISSIONS			STEP 4
				WORKSHEET W4.3
INFORMATION, DATA, AND EMISSIONS *	-- IMPACT AREAS --			
	DAMAGE	DESTRUCTION	DISCLOSURE	DENIAL
NATURAL THREATS:				
STORMS	√	√	√	√
EARTHQUAKES	√	√	√	√
FIRE	√	√	√	√
FLOOD	√	√	√	√
HURRICANE	√	√	√	√
POLLUTION	√	√	√	√
TORNADO	√	√	√	√
LIGHTNING	√	√	√	√
INTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
TERRORIST INCIDENT	√	√	√	√
BOMBING	√	√	√	√
RIOT/CIVIL DISORDER	√	√	√	√
SABOTAGE	√	√	√	√
ARSON	√	√	√	√
VANDALISM	√	√	√	√
THEFT	√	√	√	√
UNAUTHORIZED ACCESS	√	√	√	√
MISAPPROPRIATION	√	√	√	√
WIRETAPPING/EAVESDROPPING	√	√	√	√
VIRUS	√	√	√	√
TRAP DOOR	√	√	√	√
TROJAN HORSE	√	√	√	√
MASQUERADE	√	√	√	√
ERASURE	√	√	√	√
EMISSION INTERCEPTION	√	√	√	√
STRIKES	√	√	√	√
UNINTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
ACCIDENTS	√	√	√	√
OPERATIONAL/PROCEDURAL ERRORS	√	√	√	√
HARDWARE FAILURE/MALFUNCTION	√	√	√	√
SOFTWARE ERRORS	√	√	√	√
ERASURE	√	√	√	√
NEGLIGENCE	√	√	√	√
EMOTIONAL, MENTAL, HEALTH PROBLEMS	√	√	√	√
ENVIRONMENTAL THREATS:				
HEATING/COOLING SYSTEM FAILURE	√	√	√	√
POWER FLUCTUATIONS/OUTAGE	√	√	√	√
TEMPERATURE/HUMIDITY FLUCTUATIONS	√	√	√	√
STRUCTURAL FAILURE	√	√	√	√

* INFORMATION, DATA, AND EMISSIONS INCLUDE BOTH HARD-COPY AND ELECTRONICALLY STORED DATA, AND ELECTRONIC EMISSIONS.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT	THREATS TO AND VULNERABILITIES OF COMMUNICATIONS			STEP 4
				WORKSHEET W4.4
COMMUNICATIONS *	-- IMPACT AREAS --			
	DAMAGE	DESTRUCTION	DISCLOSURE	DENIAL
NATURAL THREATS:				
STORMS	√	√		√
EARTHQUAKES	√	√	√	√
FIRE	√	√	√	√
FLOOD	√	√	√	√
HURRICANE	√	√		√
TORNADO	√	√	√	√
LIGHTNING	√	√		√
INTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
TERRORIST INCIDENT	√	√	√	√
BOMBING	√	√	√	√
RIOT/CIVIL DISORDER	√	√	√	√
SABOTAGE	√	√	√	√
ARSON	√	√	√	√
VANDALISM	√	√	√	√
THEFT			√	√
UNAUTHORIZED ACCESS	√	√	√	√
MISAPPROPRIATION			√	√
WIRETAPPING/EAVESDROPPING			√	√
NEGLECT	√	√	√	√
STRIKES				√
UNINTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
ACCIDENTS	√	√	√	√
OPERATIONAL/PROCEDURAL ERRORS	√	√	√	√
HARDWARE FAILURE/MALFUNCTION	√	√	√	√
NEGLECT	√	√	√	√
ENVIRONMENTAL THREATS:				
HEATING/COOLING SYSTEM FAILURE	√	√		√
POWER FLUCTUATIONS/OUTAGE	√	√		√
TEMPERATURE/HUMIDITY FLUCTUATIONS	√	√		√
STRUCTURAL FAILURE	√	√	√	√

* COMMUNICATIONS INCLUDES ALL COMMUNICATION CAPABILITIES AND EQUIPMENT: LINES, NETWORKS, COMSEC SECURITY DEVICES, PROTECTED DISTRIBUTION SYSTEMS, PHONES, MODEMS, ETC.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT	THREATS TO AND VULNERABILITIES OF COMPUTER HARDWARE			STEP 4
				WORKSHEET W4.5a
COMPUTER HARDWARE *	- IMPACT AREAS -			
	DAMAGE	DESTRUCTION	DISCLOSURE	DENIAL
NATURAL THREATS:				
STORMS	✓	✓		✓
EARTHQUAKES	✓	✓	✓	✓
FIRE	✓	✓	✓	✓
FLOOD	✓	✓	✓	✓
HURRICANE	✓	✓		✓
POLLUTION	✓			✓
TORNADO	✓	✓	✓	✓
LIGHTNING	✓	✓		✓
INTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
TERRORIST INCIDENT	✓	✓	✓	✓
BOMBING	✓	✓	✓	✓
RIOT/CIVIL DISORDER	✓	✓	✓	✓
SABOTAGE	✓	✓	✓	✓
ARSON	✓	✓	✓	✓
VANDALISM	✓	✓	✓	✓
THEFT	✓	✓	✓	✓
UNAUTHORIZED ACCESS	✓	✓	✓	✓
MISAPPROPRIATION	✓	✓		✓
VIRUS				✓
TRAP DOOR				✓
TROJAN HORSE				✓
NEGLECT	✓	✓		✓
STRIKES				✓
UNINTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
ACCIDENTS	✓	✓	✓	✓
OPERATIONAL/PROCEDURAL ERRORS	✓	✓	✓	✓
HARDWARE FAILURE/MALFUNCTION	✓			✓
NEGLIGENCE	✓	✓	✓	✓
ENVIRONMENTAL THREATS:				
HEATING/COOLING SYSTEM FAILURE	✓	✓		✓
POWER FLUCTUATIONS/OUTAGE	✓	✓		✓
TEMPERATURE/HUMIDITY FLUCTUATIONS	✓	✓		✓
STRUCTURAL FAILURE	✓	✓	✓	✓

* COMPUTER HARDWARE INCLUDES THE CPU, PERIPHERALS, CONTROLLERS, ETC.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT	THREATS TO AND VULNERABILITIES OF COMPUTER SOFTWARE			STEP 4
				WORKSHEET W4.5b
COMPUTER SOFTWARE *	- IMPACT AREAS -			
	DAMAGE	DESTRUCTION	DISCLOSURE	DENIAL
NATURAL THREATS:				
STORMS	✓	✓		✓
EARTHQUAKES	✓	✓	✓	✓
FIRE	✓	✓	✓	✓
FLOOD	✓	✓	✓	✓
HURRICANE	✓	✓		✓
POLLUTION	✓	✓		✓
TORNADO	✓	✓	✓	✓
LIGHTNING	✓	✓		✓
INTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
TERRORIST INCIDENT	✓	✓		✓
BOMBING	✓	✓		✓
RIOT/CIVIL DISORDER	✓	✓		✓
SABOTAGE	✓	✓		✓
ARSON	✓	✓		✓
VANDALISM	✓	✓		✓
THEFT	✓	✓	✓	✓
UNAUTHORIZED ACCESS	✓	✓	✓	✓
MISAPPROPRIATION	✓	✓		✓
VIRUS	✓	✓	✓	✓
TRAP DOOR	✓	✓	✓	✓
TROJAN HORSE	✓	✓	✓	✓
MASQUERADE	✓	✓	✓	✓
ERASURE	✓	✓		✓
NEGLECT	✓	✓		✓
STRIKES	✓	✓		✓
UNINTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
ACCIDENTS	✓	✓		✓
OPERATIONAL/PROCEDURAL ERRORS	✓	✓		✓
HARDWARE FAILURE/MALFUNCTION	✓	✓		✓
ERASURE	✓	✓		✓
NEGLIGENCE	✓	✓		✓
PROGRAMMING ERRORS	✓	✓	✓	✓
ENVIRONMENTAL THREATS:				
HEATING/COOLING SYSTEM FAILURE	✓	✓		✓
POWER FLUCTUATIONS/OUTAGE	✓	✓		✓
TEMPERATURE/HUMIDITY FLUCTUATIONS	✓	✓		✓
STRUCTURAL FAILURE	✓	✓		✓

* COMPUTER SOFTWARE INCLUDES OPERATING SYSTEM SOFTWARE, APPLICATIONS SOFTWARE, UTILITIES SOFTWARE, ETC.

DEPARTMENT OF ENERGY ADP SYSTEM RISK ASSESSMENT	THREATS TO AND VULNERABILITIES OF ADP SYSTEM PROCEDURES, ADMINISTRATION AND MANAGEMENT			STEP 4
				WORKSHEET W4.6
ADP SYSTEM PROCEDURES, ADMINISTRATION AND MANAGEMENT *	- IMPACT AREAS -			
	DAMAGE	DESTRUCTION	DISCLOSURE	DENIAL
NATURAL THREATS:				
STORMS	√	√	√	√
EARTHQUAKES	√	√	√	√
FIRE	√	√	√	√
FLOOD	√	√	√	√
HURRICANE	√	√	√	√
TORNADO	√	√	√	√
INTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
TERRORIST INCIDENT	√	√	√	√
BOMBING	√	√	√	√
RIOT/CIVIL DISORDER	√	√	√	√
SABOTAGE	√	√	√	√
ARSON	√	√	√	√
VANDALISM	√	√	√	√
THEFT	√	√	√	√
UNAUTHORIZED ACCESS	√	√	√	√
NEGLECT	√	√	√	√
UNINTENTIONAL HUMAN THREATS: INSIDER OR OUTSIDER				
ACCIDENTS	√	√	√	√
OPERATIONAL/PROCEDURAL ERRORS	√	√	√	√
NEGLECT	√	√	√	√
EMOTIONAL, MENTAL, HEALTH PROBLEMS	√	√	√	√
ENVIRONMENTAL THREATS:				
POWER OUTAGE	√	√	√	√
TEMPERATURE/HUMIDITY FLUCTUATIONS	√	√	√	√
STRUCTURAL FAILURE	√	√	√	√

* PROCEDURES, ADMINISTRATION, AND MANAGEMENT INCLUDES ALL PROCEDURAL, ADMINISTRATIVE AND ORGANIZATIONAL FUNCTIONS, DOCUMENTATION AND GENERAL BUSINESS/PRACTICES THAT ARE NECESSARY TO EFFECTIVELY OPERATE/USE THE SYSTEM.



STEP 5
WORKSHEETS



**DEPARTMENT OF ENERGY
ADP SYSTEM RISK ASSESSMENT**

**COUNTERMEASURES
IDENTIFICATION AND
RISK PROFILE ACCEPTANCE**

**STEP 5
WORKSHEET
W5**

1. System Name/Identification: _____

2. SECURITY DISCIPLINE AREA	(a) ACCEPT CURRENT RISK PROFILE (YES OR NO)	(b) COUNTERMEASURES TO BE IMPLEMENTED	(c) APPROX. COST	(d) PRIORITY	(e) TARGET DATE
a. Physical Security:					
b. Personnel Security:					
c. Information Security:					
d. Communications Security:					
e. Emissions Security (TEMPEST):					
f. Computer Security (Hardware & Software):					
g. Administrative/Procedural Security and Security Management					
h. Environmental Security and Safety:					



STEP 6
EXECUTIVE SUMMARY



STEP 1

1a. GEOGRAPHIC AND ADMINISTRATIVE INFORMATION

System Name/Identification: _____
 Organization/User: _____
 DOE Facility Name: _____
 Site/Location: _____
 Facility Address: _____
 CSSO or Person Performing Risk Assessment:
 Name: _____ Location: _____
 Organization: _____ Phone No.: () _____

1b. PRIMARY SYSTEM USE

<input type="checkbox"/> Academic/Research	<input type="checkbox"/> Scientific/Technical
<input type="checkbox"/> Administration Management	<input type="checkbox"/> Manufacturing/Production
<input type="checkbox"/> Engineering/Design	<input type="checkbox"/> Other

1c. SYSTEM CONNECTIVITY

Stand Alone System: <input type="checkbox"/>	Network System:
	LAN: <input type="checkbox"/> WAN: <input type="checkbox"/>

	<input type="checkbox"/> : Open
	<input type="checkbox"/> : Closed

1d. TYPE OF SYSTEM

<input type="checkbox"/> SMALL/SIMPLE SYSTEM		<input type="checkbox"/> LARGE/COMPLEX SYSTEM	
<input type="checkbox"/> Memory Typewriter	<input type="checkbox"/> CAD/CAM/Graphics Workstation	<input type="checkbox"/> CAD/CAM/Graphics Workstation	<input type="checkbox"/> Super-Computer
<input type="checkbox"/> Word Processor	<input type="checkbox"/> Other: _____	<input type="checkbox"/> Mini-Computer	<input type="checkbox"/> Other: _____
<input type="checkbox"/> Personal Computer	_____	<input type="checkbox"/> Mainframe	_____
<input type="checkbox"/> Smart Terminal	_____		

1e. SUMMARY OF SYSTEM REPLACEMENT COSTS

<u>Replacement Costs</u>	<u>Very Low</u>	<u>Low</u>	<u>Medium</u>	<u>High</u>	<u>Very High</u>
(1) Hardware Cost:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(2) Software Cost:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(3) Data Cost:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4) Total System Cost:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

1f. STATUS OF SYSTEM BACK-UPS

	YES: All Needed Back-ups Exist	NO: Back-ups Are Needed	Identify Additional Back-ups Required: _____
• Software Back-ups	<input type="checkbox"/>	<input type="checkbox"/>	_____
• Data Back-ups	<input type="checkbox"/>	<input type="checkbox"/>	_____

2a. SENSITIVITY OR CLASSIFICATION OF SOFTWARE AND DATA

(1) SOFTWARE (APPLICATIONS, PROGRAMS):

Unclassified

Sensitive Unclassified

Classified

If Applicable, Check:

- Vital Records
- UCNI
- Privacy Act
- OOU*
- Other

- Highest Level _____
- Applicable Categories (RD, FRD, NSI, PARD) _____
- Mode of Operation _____

___%

___%

___%

(2) DATA:

Unclassified

Sensitive Unclassified

Classified

If Applicable, Check:

- Vital Records
- UCNI
- Privacy Act
- OOU*
- Other

- Highest Level _____
- Applicable Categories (RD, FRD, NSI, PARD) _____

___%

___%

___%

2b. OVERALL IMPORTANCE OF A SYSTEM, SOFTWARE, AND DATA

1. SYSTEM

	<u>Very Low</u>	<u>Low</u>	<u>Medium</u>	<u>High</u>	<u>Very High</u>
Number of Users:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Frequency of Use:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Impact If Unavailable:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. SOFTWARE

	<u>Very Low</u>	<u>Low</u>	<u>Medium</u>	<u>High</u>	<u>Very High</u>
Frequency of Use:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Impact If Unavailable:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note Additional Back-up Requirements:

3. DATA

	<u>Very Low</u>	<u>Low</u>	<u>Medium</u>	<u>High</u>	<u>Very High</u>
Frequency of Use:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Impact if Unavailable:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note Additional Back-up Requirements:

STEP 2

* Possible future category.

3. BASELINE SECURITY REQUIREMENTS REVIEW

STEP 3

(1) BLSR BY SECURITY DISCIPLINE	(a) ALL RQMTS. MET (YES OR NO)	(b) NOTED DEFICIENCY(IES)	(c) WILL DO BY	(d) COMMENTS AND/OR SUPPLEMENTARY UPGRADES
a) Physical Security:				
b) Personnel Security:				
c) Information Security:				
d) Communications Security:				
e) Emission Security (TEMPEST):				
f) Computer Security (Hardware and Software):				
g) Procedural/ Administrative Security and Security Management:				
h) Environmental Security and Safety:				

(2) Based on results of Step 1 and Step 2, are the measures in-place sufficient given:

Hardware and Software: Cost(a)

Yes

No

System Software and Data: Characteristics and Importance

Yes

No

(3) Comments: _____

4. THREAT AND VULNERABILITY ANALYSIS REVIEW

STEP 4

(1) ASSET AREA	(a) THREATS AND VULNERABILITY(IES)	(b) PROBABILITY (H,M,L)	(c) PRIORITY OF CONCERN
a) Physical (Facility):			
b) Personnel:			
c) Information, Data, and Emissions:			
d) Communications:			
e) Computer (Hardware & Software):			
f) Procedures, Administration, and Management:			
g) Operational Environment and Safety:			

5. COUNTERMEASURES IDENTIFICATIONS AND RISK PROFILE ACCEPTANCE

STEP 5

(1) SECURITY DISCIPLINE AREA	(a) ACCEPT CURRENT RISK PROFILE (YES OR NO)	(b) COUNTERMEASURES TO BE IMPLEMENTED	(c) APPROX. COST	(d) PRIORITY	(e) TARGET DATE
a) Physical Security:					
b) Personnel Security:					
c) Information Security:					
d) Communications Security:					
e) Emissions Security (TEMPEST):					
f) Computer Security (Hardware and Software):					
g) Procedural/ Administrative Security and Security Management					
h) Environmental Security and Safety:					

6. MANAGEMENT UNDERSTANDING OF RISK PROFILE AND COUNTERMEASURES REQUIRED

I/We have carefully assessed the risk(s) to the _____ system, its associated peripherals, (if applicable) its remote processing terminals, and telecommunications links. Based upon the assessment conducted by _____ (your name), the implemented security measures and/or planned corrective measures are/will be sufficient to manage the risks identified for this system.

STEP 6

Name: _____

Title: _____

Signed: _____

Date: _____

Name: _____

Title: _____

Signed: _____

Date: _____

COMMENTS: _____

GLOSSARY

The purpose of the glossary is to provide definitions and/or descriptions of terms used in this Guideline. The terms were drawn from three sources:

- (1) the DOE Computer Security Glossary, prepared by Lawrence Livermore National Laboratory and United States Air Force, HQ/SCTT, October 23, 1987;
- (2) DOE Order 1360.2A, Unclassified Computer Security Program, 5-20-88; and
- (3) DOE Order 5637.1, Classified Computer Security Program, 1-29-88.

In addition, terms for selected countermeasures were added to provide any clarifications needed by the user.

ACCEPTABLE LEVEL OF RISK A judicious and carefully considered assessment that an automatic data processing (ADP) activity or network meets the minimum requirements of applicable security directives. The assessment should take into account the value of ADP assets; threats and vulnerabilities; countermeasures and their efficacy in compensating for vulnerabilities and operational requirements.

ACCESS The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADP system. Personnel only receiving output products from the ADP system and not inputting to or otherwise interacting with the system (i.e., no "hands on" or other direct input or inquiry capability) are not considered to have ADP system access and are accordingly not subject to the personnel security requirements. Such output products, however, shall either be reviewed prior to dissemination or otherwise determined to be properly identified as to content and classification.

ACCESS CONTROL The process of limiting access to the resources of a system to authorized users, programs, processes, other systems, or networks.

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 quality or state which enables violations or attempted violations of ADP system security to be traced to individuals who may then be held responsible.

ACCREDITATION The documented authorization, by the designated authority, granted to an organization or individual to operate an ADP system or network in

a specific environment to process, store, transfer or provide access to classified information.

ADMINISTRATIVE SECURITY The management constraints; operational, administrative, and accountability procedures; and supplemental controls established to provide an acceptable level of protection for data. Synonymous with PROCEDURAL SECURITY.

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

ADP SECURITY Measures required to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of ADP systems and data, and denial of service to process data. ADP security includes consideration of all hardware/software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the ADP system and for the data or information contained in the system.

ADP SYSTEM An assembly of computer hardware, firmware, 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), or other stand-alone or special computer systems.

ADP SYSTEM SECURITY Includes all hardware/software functions, characteristics, and features, operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities, and, the management constraints, physical structures, and devices; personnel and communication controls needed to provide an acceptable level of protection for classified material to be contained in the computer system.

ANNUAL LOSS EXPECTANCY (ALE) The ALE of an ADP system or activity is the expected yearly dollar value loss from the harm to the system or activity by attacks against its assets.

APPLICATION SOFTWARE (FUNCTIONAL) Routines and programs designed by, or for system users and customers. Through the use of available automated system equipment and basic software, application software completes specific, mission-oriented tasks, jobs, or functions. It can be either general purpose packages, such as demand deposit accounting, payroll, machine tool control, and so forth, or specific application programs tailored to complete a single or limited number of user functions, for example, base-level personnel, depot maintenance, missile or satellite tracking, and so forth. Except for general purpose packages that are acquired directly from software vendors or from the original equipment manufacturers, this type of software is generally developed by the user either with in-house resources or through contract services.

APPROVAL TO OPERATE Concurrence by the DAA that a satisfactory level of security has been provided (minimum requirements are met and there is an acceptable level of risk). It authorizes the operation of an automated system

or network at a computer facility. Approval results from an analysis of the computer facility, automated system, and automatic data system certifications and the operational environment of the automated system entity by the DAA. See ACCREDITATION.

AUDIT TRAIL A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in the path of a transaction from its inception to output of final results.

AUTHENTICATION The act of identifying or verifying the eligibility of a station, originator, or individual to access information. This measure is designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, 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.

AUTOMATED SYSTEM SECURITY All security features needed to provide an acceptable level of protection for hardware; software; and classified, sensitive unclassified or critical data, material, or processes in the system. It includes: all hardware and software functions, characteristics and features, operational procedures, accountability procedures, access controls at all computer facilities, (includes those housing mainframes, terminals, minicomputers, or microcomputers), management constraints, physical protection, control of compromising emanations (TEMPEST), personnel and communications security (COMSEC), and other security disciplines.

AVAILABILITY That computer security characteristic that ensures the computer resources will be available to authorized users when they need them. This characteristic protects against denial of service.

BACKUP OR REDUNDANCY The provision of facilities, logical or physical, to speed the process of Restart and Recovery following failure. Such facilities might include duplicated files or transactions, periodic dumping of core or backing storage contents, duplicated processors, storage devices, terminals or telecommunications hardware, and the switches to effect a changeover.

BACKUP PROCEDURES The provisions made for the recovery of data files and program libraries, and for restart or replacement of ADP equipment after a system failure or disaster.

BASE AND BOUNDS REGISTERS Identify upper and lower limits of a protected area to restrict access to other areas.

BASELINE SECURITY REQUIREMENTS A description of minimum requirements provided for a system to maintain an acceptable level of security. The baseline does not necessarily constitute one document but may be an accumulation of the security requirements stated in several documents.

BIOMETRIC The use of specific quantities that reflect unique personal characteristics (such as a fingerprint, an eye blood vessel print, or a voice print) to validate the identify of users.

BROWSING An unstructured search through storage in hope of obtaining otherwise inaccessible information.

CALL BACK A procedure for identifying a terminal dialing into a system by disconnecting the caller and reestablishing the connection by the computer system dialing the telephone number of the calling terminal. Synonymous with **DIAL BACK**.

CERTIFICATION A statement that specifies the extent to which the security measures meet specifications. Certification is based on the results of the risk assessment and security tests performed. It does not necessarily imply a guarantee that the described system is impenetrable.

CHAIN OF CUSTODY CONTROLS Measures implemented to control the chain of custody for hardware or software from manufacturer, through the logistic support system, down to the user site to ensure that no modification or tampering can take place.

CHECKSUMS A digit added to each number in a coding system which allows for detection of errors in the recording of the code numbers. Through the use of the check digit and a predetermined mathematical formula, recording errors such as digit reversal can be noted. Synonymous with parity bit.

CHOKER PACKETS Packet sent to sender to advise sender to reduce the traffic sent to a specific destination by X percent.

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

CLEARING The overwriting of classified information on magnetic media such that the media may be reused. This does not lower the classification level of the media.

CLEARING MAGNETIC MEDIA A procedure used to erase the sensitive or classified information stored on the media, but lacking the totality of a declassification procedure.

COMMUNICATIONS SECURITY, (COMSEC) The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information.

COMMUNITY OF INTEREST SEPARATION Security control mechanism which provides for the creation of logical subnets with disjoint non-hierarchical mandatory access control categories, and protection of control information from active wiretapping.

COMPARTMENTALIZATION The isolation of the operating system, user programs, and

data files from one another in main storage in order to provide protection against unauthorized or concurrent access by other users or programs. This term also refers to the division of sensitive data into small, isolated blocks for the purpose of reducing risk to the data.

COMPARTMENTED MODE SECURITY The mode of operation which allows the system to process two or more types of compartmented information (information requiring a special authorization) or any one type of compartmented information with other than compartmented information. In this mode, all system users need not be cleared for all types of compartmented information processed, but must be fully cleared for at least Top Secret information for unescorted access to the computer.

COMPROMISE An unauthorized disclosure or loss of sensitive information that may result in its unauthorized disclosure, modification, or destruction.

COMPUTER ABUSE Willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation. Levels of computer abuse are:

Minor abuse - acts that represent management problems, such as, printing calendars or running games, that do not impact system availability for authorized applications;

Major abuse - unauthorized use (possibly criminal), denial of service, and multiple instances of minor abuse to include waste;

Criminal act - fraud, embezzlement, theft, malicious damage, misappropriation, conflict of interest, and unauthorized access to classified data.

COMPUTER FACILITY Physical resources that include structures or parts of structures to house and support capabilities. For small computers, stand-alone systems, and word processing equipment, it is the physical area where the computer is used.

COMPUTER FRAUD Computer-related crimes involving misrepresentation or alteration of data in order to obtain something of value (usually for monetary gain). A computer system must have been involved in the perpetration or cover-up of the act, or series of acts. A computer system might have been involved through improper manipulation of (1) input data; (2) output or results; (3) applications programs; (4) data files; (5) computer operations; (6) communications; or (7) computer hardware, systems software, or firmware.

COMPUTER NETWORK A complex consisting of two or more interconnected computers.

COMPUTER SECURITY The protection of the information and physical assets of a computer system. The protection of information aims to prevent the unauthorized disclosure, manipulation, destruction or alteration of data. The protection of physical assets implies security measures against theft, destruction or misuse of equipment, i.e., processors, peripherals, data storage media, communication lines and interfaces.

CONFIGURATION MANAGEMENT The management of changes made to a system's hardware, software, firmware, and documentation throughout the development and operational life of the system.

CONTINGENCY PLAN(S) A plan for emergency response, backup operations, and post-disaster recovery maintained by an ADP activity as a part of its security program. A comprehensive, consistent statement of all the actions to be taken before, during, and after a disaster, along with documented, tested procedures that, if followed, will ensure the availability of critical resources and that will facilitate maintaining the continuity of operations in an emergency situation.

CONTROLLED AREA An area or space to which access is physically controlled.

CONTROLLED SECURITY MODE An automated system is operating in the controlled security mode when at least some users with access to the system have neither the required security clearance nor a need-to-know for all classified material contained in the system. However, the separation and control of users and classified material are not accomplished by the operating system as in the Multilevel Security Mode. Instead, it is accomplished by the implementation of security measures which reduce or eliminate most system software vulnerabilities.

CONTROLLED SPACE The three-dimensional space surrounding equipment that processes national security information within which unauthorized personnel are 1) denied unrestricted access and 2) enter escorted by authorized personnel or under continual physical or electronic surveillance.

COUNTERMEASURE Any action, device, procedure, technique, or other measure that reduces the vulnerability of a system (e.g., hardware, software, personnel, physical, communications or administrative).

CROSSCHECK OR SUMMARY RECONCILIATION This control involves the periodic exchange of reports between communicating terminals of message types and counts received for comparison. Also, end-of-day totals for all traffic may be summed across terminals for comparison to ensure that they equal the system message count maintained in a separate register.

DATA INTEGRITY The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or intentional modification, disclosure, or destruction.

DEDICATED SECURITY MODE The mode of operation in which the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. In this mode, all users have the clearance, formal access approval, and need-to-know for all data handled by the system.

DENIAL OF SERVICE Action or actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes the unauthorized destruction, modification, or delay of service.

DESIGNATED APPROVING AUTHORITY (DAA) A designated official who has the

authority and the responsibility to make the management decision to accept or not accept the security safeguards prescribed for an ADP system(s) or network and for issuing an accreditation statement that records the decision to accept those safeguards.

DIGITAL SIGNATURES Digital signatures allow a recipient of a data unit to prove the source and integrity of the data unit and protects against forgery, for example, by the recipient. A digital signature is created by appending data to, or performing a cryptographic transformation of, a data unit.

DISCRETIONARY PROTECTION Access control that identifies individual users and their need-to-know and limits users to the information that they are allowed to see. It is used on systems that process information with the same level of sensitivity.

EMISSION SECURITY, (EMSEC) That component of communications security which results from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

ENCRYPTION Transforming a text into code in order to conceal its meaning.
End-to-End Encryption: Encryption of information at the origin within a communications network and postponing decryption to the final destination point. **Line Encryption:** The application of on-line crypto-operations to a link of a communications system so that all information passing over the link is encrypted.

END-TO-END ENCRYPTION Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system.

ERASURE A process by which a signal recorded on magnetic media is removed. Erasure is accomplished in two ways: (1) by alternating current erasure, the information is destroyed by applying an alternating high/low current to the media, or (2) by direct current erasure, the media are saturated by applying a unidirectional current.

ERROR DETECTING AND CORRECTING A system employing an error detecting code and so arranged that a signal detected as being in error automatically initiates a request for retransmission.

ERROR RECOVERY Mechanisms that allow the recovery from transmission errors, node failures, invalid protocol usage, traffic jams, missing packets, and disrupted sessions.

ESCORT(S) Duly designated personnel who have appropriate clearances and access authorizations for the material contained in the system and are sufficiently knowledgeable to understand the security implications of and to control the activities and access of the individual being escorted.

EVALUATED PRODUCTS LIST, (EPL) A documented inventory of commercially available trusted computer hardware and software that has been evaluated against the Department of Defense Trusted Computer System Evaluation Criteria by the National Computer Security Center.

EVENT DETECTION AND HANDLING Mechanisms that provide for the identification of specific events or situations and initiate appropriate action upon detection of the event or situation.

EXECUTION DOMAINS Processor is divided into states to provide isolation support. A two state processor has a user state and a supervisor state. Supervisor state has more privileges than user state. Multiple state machines may use multiple execution domains. The program executing in an inner level has free use of the instructions in the outer level state; however, a program executing in the outer level does not have use of the instructions in the inner level. CPU knows which domain is in control and only operations specified as allowable can take place.

FAULT TOLERANCE Mechanisms that provide a capability to deal with network failures and to maintain continuity of operations of a network including the following features: error/fault detection, fault treatment, damage assessment, error/failure recovery, component/segment crash recovery, and whole network crash recovery.

FILE PROTECTION The aggregate of all processes and procedures established in an automated system and designed to inhibit unauthorized access, contamination, or elimination of a file.

FIRMWARE Software that is permanently stored in a hardware device which allows reading of the software but not writing or modifying. The most common device for firmware is read only memory (ROM).

FLOW CONTROL Mechanism that requires sender to stop sending at some point and wait for an explicit go-ahead message, or permit the receiver to simply discard messages at will.

FOR OFFICIAL USE ONLY (FOUO) DATA Data that is unclassified official information of a sensitive, proprietary, or personal nature which must be protected against unauthorized public release.

HACKER Originally, a computer enthusiast who spent significant time learning the functions of the computer without benefit of formal training (and often without the technical manuals) by trying combinations of commands at random to determine their effect. Common usage today is from the press, which uses the word to describe people who "break into" computers for various purposes.

HANDSHAKING A preliminary exchange of predetermined signals performed by modems and/or terminals and computers to verify that communication has been established and can proceed.

HANDSHAKING PROCEDURES A dialogue between a user and a computer, a computer and another computer, a program and another program for the purpose of identifying a user and authenticating identity. A sequence of questions and answers is used based on information either previously stored in the computer or supplied to the computer by the initiator of the dialogue.

HARDWARE The electric, electronic, and mechanical equipment used for processing data.

HARDWARE PROTOCOL VERIFICATION Hardware protocol verification can be applied to help ensure that the host is in contact with the right terminal (the one it thinks it is). The terminal identity can be made software invariant by storing it in a chip from where it is taken to answer a poll or select.

IMPERSONATION An attempt to gain access to a system by posing as an authorized user. Synonymous with MASQUERADING and MIMICKING.

INFORMATION RESOURCES MANAGEMENT The planning, budgeting, organizing, directing, training, and control associated with government information. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and technology.

INFORMATION SECURITY The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

INFORMATION SYSTEMS SECURITY The protection afforded to information systems in order to preserve the availability, integrity, and confidentiality of the systems and information contained within the systems. Such protection is the application of the combination of all security disciplines which will, at a minimum, include COMSEC, TEMPEST, computer security, OPSEC, information security, personnel security, industrial security, resource protection, and physical security.

INTEGRITY That computer security characteristic that ensures that computer resources operate correctly and that the data in the data bases are correct. This characteristic protects against deliberate or inadvertent unauthorized manipulation of the system and ensures and maintains the security of entities of a computer system under all conditions.

INTELLIGENCE INFORMATION Classified information defined as intelligence information by Director of Central Intelligence Directive 1/16.

INTERIM APPROVAL The temporary authorization granted an information system to process sensitive or classified information based on preliminary results of a comprehensive security evaluation of the information system.

INTERNAL CONTROLS The plan of organization and all of the methods and measures adopted within an agency to safeguard its resources, assure the accuracy and reliability of its information, assure adherence to applicable laws, regulations and policies, and promote operational economy and efficiency.

INTERNAL CONTROL DOCUMENTATION Written policies, organization charts, procedural write-ups, manuals, memoranda, flowcharts, decision tables, completed questionnaires, software, and related written materials used to describe the internal control methods and measures, to communicate responsibilities and authorities for operating such methods and measures, and to serve as a reference for persons reviewing the internal controls and their functioning.

KEY In cryptography, a symbol or sequence of symbols (or electrical or mechanical correlates of symbols) which control the operations of encryption

and decryption.

KEY MANAGEMENT Specific manual and computer procedures for the generation, dissemination, replacement, storage, archive, and destruction of secret keys that control encryption or authentication processes.

LABEL A piece of information that represents the security level of an object and that describes the sensitivity of the information in the object.

LEAST PRIVILEGE The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

LIMITED ACCESS SECURITY MODE The type of data being processed is categorized as unclassified and requires the implementation of special access controls to restrict the access to the data only to individuals who by their job function have a need to access the data.

LIVENESS CHECKS Verification that a network component(s) is functioning properly.

LOCKS AND KEYS MEMORY PROTECTION Locks (identifiers assigned to areas of real memory) restrict access to memory by requiring that the user or programmer supply the key to unlock memory and allow access.

LOGIC BOMB A resident computer program that, when executed, checks for particular conditions or particular states of the system, which when satisfied triggers the perpetration of an unauthorized act.

LOGOFF/LOG OFF Procedure used to terminate connections.

LOGON/LOG ON Procedure used to establish the identity of the user, and the levels of authorization and access permitted.

LOOPHOLE An error of omission or oversight in software or hardware that permits circumventing the access control process.

MALICIOUS LOGIC Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose. An example is a Trojan horse.

MANDATORY ACCESS CONTROL SECURITY MODE A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity.

MARKING The process of placing a sensitivity designator (e.g., "confidential") with data such that its sensitivity is communicated. Marking is not restricted to the physical placement of a sensitivity designator, as might be done with a rubber stamp, but can involve the use of headers for network messages, special fields in databases, etc.

MASQUERADING An attempt to gain access to a system by posing as an authorized user. Synonymous with MIMICKING and IMPERSONATION.

MEDIA The peripheral devices (physical components) used for the storage of data, such as tape reels, floppy diskettes, etc.

MOCKINGBIRD A computer program or process which mimics the legitimate behavior of a normal system feature (or other apparently useful function) but performs malicious activities once invoked by the user.

MODES OF OPERATION The definition of the security environment and approved methods of operating a system.

MULTILEVEL DEVICE A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (i.e., machine-readable or human-readable) as the data being processed.

MULTILEVEL SECURITY MODE A mode of operation that provides a capability for various levels and categories or compartments of data to be concurrently stored and processed in an automated system and permits selective access to such material concurrently by users who have differing security clearances and need-to-know. Internal controls, as well as personnel, physical, and administrative controls, separate users and data on the basis of security clearance. The internal security controls must be thoroughly demonstrated to be effective in preventing unauthorized access to information.

NATIONAL SECURITY DECISION DIRECTIVE 145 (NSDD-145) Signed by President Reagan on 17 September 1984, this directive is entitled, "National Policy on Telecommunications and Automated Information Systems Security." It provides initial objectives, policies, and an organizational structure to guide the conduct of national activities toward safeguarding systems that process, store, or communicate sensitive information; establishes a mechanism for policy development; and assigns implementation responsibilities.

NEED-TO-KNOW The necessity for access to, knowledge of, or possession of certain information required to carry out official duties. Responsibility for determining whether a person's duties require that possession of or access to such information and whether the individual is authorized to receive it rests upon the individual having current possession, knowledge, or control of the information involved and not upon the prospective recipient(s).

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.

NETWORK FRONT END A device that implements the necessary network protocols, including security related protocols, to allow a computer system to be attached to a network.

NETWORK WEAVING Network weaving is a technique using different communication networks to gain access to an organization's system. For example, a perpetrator [...] makes a call through AT&T, jumps over to Sprint, then to MCI, and then to Tymnet. The purpose is to avoid detection and trace-backs to the

source of the call.

NOFORN No foreign dissemination. This term indicates that the information contained in the document must not be released to foreign nationals.

NOTARIZATION The registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery.

OPERATIONS SECURITY (OPSEC) The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

OVERWRITE PROCEDURE A procedure to remove or destroy data recorded on ADP magnetic storage media by recording patterns of unclassified data over or on top of the data stored on the media.

OWNER OF DATA The individual or group that has responsibility for specific data types, and that is charged with the communication of the need for certain security-related handling procedures to both the users and custodians of this data.

PARTITIONED SECURITY MODE A mode of operation wherein all personnel have the clearance but not necessarily formal access approval (need-to-know) for all information handled by the system. This encompasses the Compartmented Security Mode.

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

PASSWORD SYSTEM A part of an ADP system that is used to authenticate a user's identity. Assurance of unequivocal identification is based on the user's ability to enter a private password that no one else should know.

PENETRATION The successful unauthorized access to an automated system.

PENETRATION TESTING The use of teams consisting of data processing, communications, and security specialists to attempt to penetrate a system for the purpose of identifying any security weaknesses.

PERIODS PROCESSING Intervals of time when security environments are temporarily established for processing information. For example, an automated system could process Top Secret in the dedicated security mode during one period, both Confidential and Secret in the controlled security mode in a second period, and only unclassified material in a third period. The system is purged of all information and brought to a secure state when transitioning from one period to the next. There will be users during the new period who do not have clearance and need-to-know for information processed during the previous period.

PERSONAL DATA Any unique data used in the system of records to locate or retrieve an individual's record. Information subject to the Privacy Act of 1974. These data may include, but is not limited to, education, financial

transactions, medical history, qualifications, service data, criminal or employment history which ties the data to the individual's name, or an identifying number, symbols, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

PERSONNEL SECURITY The procedures established to ensure that all personnel who have access to any classified or sensitive information have the required authorizations and the appropriate clearances.

PHYSICAL CONTROL SPACE/ PHYSICALLY CONTROLLED SPACE (PCS) The spherical space surrounding electronic equipment used to process information which is under sufficient physical control to stop intercept of compromising emanations. It is usually expressed in meters and can be controlled by fences, guards, patrols, walls, and so forth. The exact method of securing the PCS may vary depending upon resources available.

PHYSICAL SECURITY The use of locks, guards, badges, alarms, and similar measures (alone or in combination) to control access to the classified ADP facility, system and related equipment and to protect them from espionage, theft, misuse, abuse, or damage.

PIGGYBACK The gaining unauthorized access to a system via another user's legitimate connection.

PREFERRED PRODUCTS LIST (PPL) A list of commercially produced equipments that meet TEMPEST and other requirements prescribed by NSA.

PRIORITY INDICATOR A group of characters that indicate the relative urgency of a message and thus its order of transmission.

PRIVACY PROTECTION The establishment of appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of data records and to protect both security and confidentiality against any anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained.

PROCEDURAL SECURITY The management constraints; operational, administrative, and accountability procedures; and supplemental controls established to provide protection for sensitive and classified information.

PROPRIETARY DATA Data that is created, used, and marketed by individuals having exclusive legal rights.

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.

PSEUDO-FLAW An apparent loophole deliberately implanted in an operating system program as a trap for intruders.

RECONFIGURATION Capability to reconfigure the network to provide network software maintenance and program downloading to network nodes for software

distribution, and removing failed or faulty components and replacing with replaced components can isolate and/or confine network failures, accommodate the addition and deletion of network components, and circumvent a detected fault.

RECOVERY PROCEDURES The actions necessary to restore a system's computational capability and data files after a system failure or penetration.

RED/BLACK ENGINEERING The concept that telecommunications circuits, components, equipment, and systems which handle classified plain-language information in electrical signal form (RED) be separated from those which handle encrypted or unclassified information (BLACK).

RELIABILITY The probability of a given system performing its mission adequately for a period of time under the expected operating conditions.

REMOTE TERMINAL AREA Remote computer facilities, peripheral devices, or terminals which are located outside the central computer facility.

RESTRICTED AREA Any area to which access is subject to special restrictions or controls for reasons of security or safeguarding of property or material.

RISK The probability that a particular threat will exploit a particular vulnerability of the Automated Information System or telecommunications system.

RISK ANALYSIS An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence.

RISK ASSESSMENT A study of the vulnerabilities, threats, likelihood, loss or impact, and effectiveness of security measures. Managers use the results of a risk assessment to identify security requirements and/or enhancements over the life cycle of a system.

RISK MANAGEMENT The total process of identifying, controlling, and eliminating or minimizing uncertain events affecting system resources. It includes risk assessment; cost benefit analysis; countermeasures selection; implementation; test, and evaluation; and overall security review.

ROUTING CONTROL Routing control consists of applying rules to the routing process so as to chose or avoid specific networks, links, or relays.

SANITIZATION The elimination of classified information from magnetic media to permit the reuse of the media at a lower classification level or to permit the release to uncleared personnel or personnel without the proper information access authorizations.

SANITIZE To erase or overwrite classified data stored on magnetic media for the purpose of declassifying the media.

SECURE OPERATING SYSTEM An operating system that effectively controls hardware and software functions in order to provide the level of protection appropriate to the value of the data and resources managed by the operating system.

SECURITY AREA A physically defined space containing classified matter (documents or material) subject to physical protection and personnel access controls.

SECURITY GUARD A special purpose device used to separate two systems or components which are not fully trusted to communicate securely.

SECURITY KERNEL Software designed into a system that monitors all access within the system and (in theory) cannot be tampered with or bypassed.

SECURITY MODE A secure mode of operation in which the approving authority accredits a system to operate. Inherent with each of the security modes are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the system.

SECURITY SAFEGUARDS The protective measures and controls that are prescribed to meet the security requirements specified for an AIS. Those safeguards may include but are not necessarily limited to: hardware and software security features, operations procedures, accountability procedures, access and distribution controls, management constraints, personnel security, physical structures, areas, and devices.

SECURITY TEST AND EVALUATION (ST&E) An examination and analysis of the security safeguards of an AIS as they have been applied in an operational environment to determine the security posture of the AIS.

SENSITIVE COMPARTMENTED INFORMATION (SCI) Intelligence information requiring special controls indicating restricted handling.

SENSITIVE UNCLASSIFIED INFORMATION AND DATA Sensitive unclassified information is plain text or machine encoded data requiring protection because of statutory or regulatory restrictions and/or because of the magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information (e.g., personal data, proprietary information, mission essential information, sensitive energy information, sensitive financial/supply data, risk or vulnerability assessment data, security program related information, any data not releasable under the Freedom of Information Act, and other unclassified information, the loss of which could adversely affect the vital interest of the United States).

SEQUENCE NUMBERING The numerical ordering of all traffic in the network to protect against duplication or loss of messages on the line as well as insertion of a false message into a circuit by an intruder simulating the identity of an authorized user.

SOFTWARE SECURITY Those general purpose (executive, utility, or software development tools) and applications programs, and routines which protect data handled by an ADP system and its resources.

SPOOFING The deliberate act of inducing a user or a resource into taking an incorrect action.

STAND ALONE, SINGLE-USER SYSTEM A system that is physically and electrically

isolated from all other systems, and is intended to be used by one person at a time, with no data belonging to other users remaining in the system (e.g., a personal computer with removable storage media such as a floppy disk).

SYNCHRONIZED CLOCKS Mechanism that may be used to provide "liveness" assurance in support of authentication.

SYSTEM An assembly of computer hardware, software, or firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, controlling or receiving data with a minimum of human intervention.

SYSTEM HIGH SECURITY MODE The mode of operation in which the computer system and all of its connected peripheral devices and remote terminals are protected in accordance with the requirements for the highest security level of material contained in the system at that time. All personnel having access to the system have a security clearance, but not a need-to-know, for all material then contained in the system.

SYSTEM INTEGRITY The state that exists when there is complete assurance that under all conditions an ADP system is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms, and data integrity.

SYSTEM SECURITY OFFICER (SSO) The person(s) responsible for ensuring that security is provided for and implemented throughout the life cycle of an AIS from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal.

TAGGED MEMORY Every word is tagged with some attribute such as mode, type, or security level which CPU interprets and grants or denies access.

TELECOMMUNICATIONS The preparation, transmission, communication, or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

TEMPEST The study and control of spurious electronic signals emitted by electrical equipment.

TEMPEST CONTROL ZONE The contiguous space which surrounds equipment and distribution systems and is under sufficient physical and technical control to preclude interception of compromising emanations. Sufficient physical and technical control is the degree of control that enables the security forces responsible for protecting a controlled space to detect, investigate and remove any person or device of a suspicious nature which is detected therein.

THREAT ADP Any circumstance or event with the potential to cause harm to the system or activity in the form of destruction, disclosure, and modification of data, or denial of service. A threat is a potential for harm. The presence of a threat does not mean that it will necessarily cause actual harm. Threats exist because of the very existence of the system or activity and not because of any specific weakness. For example, the threat of fire exists at all facilities, regardless of the amount of fire protection available.

TIME BOMB In computer security, a variant of the Trojan horse in which malicious code is inserted to be triggered later.

TIME STAMPING Attaching a time indicator to a data unit in order to establish the time sequence of data transmitted or may be used in conjunction with encipherment to authenticate the validity of a data unit.

TRAFFIC PADDING Traffic padding involves generating spurious instances of communication, spurious data units and/or spurious data within data units. Traffic padding may be used to provide various levels of protection against traffic analysis.

TRAP DOOR A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some innocent-appearing manner (e.g., special "random" key sequence at a terminal). Software developers often introduce trap doors in their code that enable them to re-enter the system and perform certain functions.

TROJAN HORSE A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity. For example, making a "blind copy" of a sensitive file for the creator of the Trojan horse.

TRUSTED PRODUCTS Products certified by Director, NCSC for inclusion on the Evaluated Products List (EPL).

USER ID A unique symbol or character string that is used by a system to only identify a user.

VIRUS A program or set of instructions written by malicious programmers intent on destroying information and/or overloading system operations in other computers. A virus can enter a system surreptitiously through telephone lines, enter by use of exchanged memory disks, or be hidden among legitimate information.

VULNERABILITY A weakness in system security procedures, hardware design, internal controls, etc., that could be exploited to gain unauthorized access to classified or sensitive information or disrupt processing.



**ANNOTATED BIBLIOGRAPHY
FOR THE
DOE RISK ASSESSMENT GUIDELINE**

The following bibliographic section was compiled to provide citations and brief annotations of articles in computer security and risk assessment that would be useful as supplemental resources to the users of the DOE Risk Assessment Guideline. The search conducted covered the last 5 years (1983-1988) with the objective of providing titles of relevant, recent publications on subjects of interest to the user audience. The topical areas searched are listed below. On occasion, a citation of interest was identified, but the article itself could not be located for review and annotation. However, its title was still included in the bibliography in an effort to provide a comprehensive listing of potentially useful articles. In addition, the titles of selected security-related periodicals and source books are also listed, without specific reference to an individual article, in order to identify sources of general utility in conducting future risk assessments.

Editor's Note: Bibliographic entries are grouped by category as follows: Risk Assessment: General, Risk Assessment: Computer Based Tools, Threats and Vulnerabilities, Countermeasures: Equipment/Technology, Countermeasures: Procedures, Networks, Viruses and Other Related Threats, Risk Management, Certification and Accreditation, Other U.S. Government Computer Security Publications.

BIBLIOGRAPHY

RISK ASSESSMENT: GENERAL

Brown, Rex, V. "Diffuse Risks from Adversarial Sources: An Emerging Field of Risk Analysis." Decision Science Consortium, Inc. This paper discusses the impact of multiple (diffuse) threats targeted against a specific asset or set of assets, and presents a model for exploring the range and variety of their potential impacts. The article suggests the need for using qualitative judgement as part of the risk assessment model-building process.

Burr, E.H. and Elder, R.L. "Proposal of a Simple ADP Security Cost/Risk Methodology." DOE 11th Computer Security Group Conference. May 3-5, 1988. Kansas City, Missouri. This paper describes a simple, straight-forward approach to conducting a risk/cost analysis that, once completed, provides guidance as to whether a countermeasure should be implemented based on the level of risk involved (Very Low to Very High).

Camp, John. "A Physical Security Risk Assessment of Microcomputing at the FAA." Computer Security Newsletter. May/June, 1986. This article describes the results of a 1985 computer risk analysis done by the FAA in the New England region. The article presents the findings of a 28-office physical security risk analysis, and identifies the numerous deficiencies and lax approaches to security and safety at these locations. A list of specific, cost-effective solutions are presented as action items, along with general recommendations for improving the physical security profiles of these sites.

Clark, Clara. "Risk Analysis for the Morgantown Energy Technology Center." DOE 7th Computer Security Group Conference. April 10-12, 1984. New Orleans, Louisiana. This paper describes a computer security risk analysis software tool developed by the Morgantown Energy Technology Center used to identify risks and necessary countermeasures as applied to the unclassified computer security program.

Guarro, Sergio B., Garcia, Bael A., Wood, Charles C., and Prassions, Peter G. Livermore Risk Analysis Methodology: A Quantitative Approach to Management of the Risk Associated with the Operation of Information Systems Computer and Communications Security Conference. Lawrence Livermore National Laboratory. Report No.: UCRL-95133; CONF-8610255-1. August 14, 1986.

Guarro, Sergio B. Livermore Risk Analysis Methodology: A Structured Decision Analytic Tool for Information Systems Risk Management. Lawrence Livermore National Laboratory. Report No.: UCRL-96032; CONF-8611117-4. January 16, 1987.

Helsing, Cheryl H. "Application Risk Assessment and Controls Selection." 1986 Datapro. IS20-300-101. April 1986. This report identifies vulnerabilities in information processing applications, ranks vulnerabilities by severity, assists you in selecting appropriate countermeasures, and facilitates obtaining management's acceptance of the residual risk.

Henrion, Max and Morgan, M. Granger. "A Computer Aid for Risk and Other Policy Analysis." Risk Analysis. Vol 5. No. 3. 1985. This article suggests several

possible approaches for improving the quality of currently practiced approaches to quantitative risk analysis. Several key steps are outlined, including encouraging higher standards through greater use of peer review and through developing computer tools that make it easier to construct and utilize models for use in the process.

Hoffman, Lance J. Computer Security Risk Analysis: Problems and Issues. Report GWU-IIST-86-04. Department of Electrical Engineering and Computer Science. The George Washington University. March 1986. This report discusses several issues relevant to computer security risk analysis, to include: standard definitions, risk communications, need for test beds and baseline studies, case data collection, desirability of a general risk model, lack of matrices, difficulties in transferring knowledge between the fields of risk analysis and computer security, and the appropriateness of various efforts to automate the risk analysis process.

Hoffman, Lance J., Cook, Janet M., and Mayfield, Terry. Module for Risk Analysis. This module provides an introduction to the basic principles of risk analysis and is intended to be used as part of an upperlevel software engineering course. Topics include benefits, limitations, and costs of risk analysis; procedures for risk identification and control; and tools available to the software engineer.

Hoffman, Lance J. "Risk Analysis and Computer Security: Bridging the Cultural Gaps." Proceedings of 9th National Computer Security Conference. 15-18 September, 1986. This article discusses specific problems which currently limit the effectiveness of computer security risk analysis.

Jackson, Carl, B. "Making Time for DP Risk Analysis." Security World. March 1986. This article discusses the use of quantitative analysis for use in circumstances where threats have already been addressed through already proven countermeasures.

Jacobson, Robert V., Weissleader, Howard, Arroyo, and James, M. "Low-Cost Risk Analysis A Success." Government Computer News. June 20, 1986, pg. 39. This article describes how a large federal agency has successfully combined a questionnaire and software analysis to evaluate ADP security concerns at its state offices for about one-third the cost of a standard analysis.

Miller, Donald G. "Risk Assessment in Bank Operations: State-of-the-Art." Magazine of Bank Administration, Vol. 61, No. 1. January 1985, pgs. 26-28, 30. This article outlines eight different approaches used in risk assessment of bank operations, to include risk management and various, risk assessment techniques (e.g., the "Illinois Treatment," the "Courtney Thesis", the control matrix, use of threat scenarios, bracketing, checklists, analysis programs).

Minutes of the Federal Information Systems Risk Analysis Workshop. 22-24 January, 1985. Air Force Computer Security Program Office, Gunter AFS, Alabama. [Available through Defense Technical Information Center, Alexandria, VA].

Risk Analysis. An International Journal. An Official Publication of the Society for Risk Analysis. Plenum Press. New York and London

"Risk Analysis Report for the Staffing Data Base System." Office of Strategic Planning and Integration. June 16, 1986. This report describes the results of a pilot risk analysis conducted on the Staffing Data Base System (SDBS). The objectives of this analysis were: 1) to establish a risk analysis methodology for use throughout the system, 2) to serve as a benchmark in evaluating risk analysis software products, and 3) to fulfill the requirements of OMB Circular A-130 and other security directives that mandate periodic risk analysis.

Santilli, Joseph V. "Sample Qualitative Risk Assessment for Small Systems," Center for Computer Security News. Vol 6. No. 3, December 1987. This article describes several risk assessment approaches that are now outdated, and presents a simple form for use in qualitative assessments of small systems.

Schweitzer, James A. "Computing Security Risk Analysis." Security Management. August 1981. pgs. 104-106. This article describes the basic flaws involved in conducting a security risk assessment by committee.

"Security Assessment Questionnaire: The IBM Approach." 1986 Datapro IS15-325-101. November 1986. This report provides guidance in 3 key areas: (1) assessing and developing security programs at an installation; (2) identifying security areas that need management attention; and (3) conducting a detailed evaluation of current security policies.

Snow, David W. "Mission-Based Method Best for Analyzing System Risks." Government Computer News. February 13, 1987, pg. 55. This article discusses the differences between threat-based and mission-based risk assessment methodologies.

Wade, James R. "The Basics of EDP Risk Assessment." Security Management. March 1982. pgs. 56-70. This article discusses the importance of viewing risk to an EDP center in terms of the total assets that comprise that center: hardware, software, communications, personnel, documents and media, procedures, and operating environment.

Wong, Kenneth K. Computer Security: Risk Analysis and Control. Rochelle Part, NJ. Hayden Book Co., Inc., 1977. This book provides detailed tables and matrices for use in identifying applicable risks to an ADP environment, and the numerous approaches available for implementation as countermeasures.

RISK ASSESSMENT: COMPUTER BASED TOOLS

"All About Risk Analysis Software." 1986 Datapro. IS21-001-101. March 1986. This report provides product summaries for 8 software products for risk analysis from 7 vendors.

Brown, Nander. "Automated Tools Help SBA Build Risk Assessments." Government Computer News. April 29, 1988. p. 42. This article describes the Small Business Administration's approach to using a variety of available software tools to facilitate the risk assessment process.

Cox, Jr. Louis A. "ATAM: A Personal Computer Modeling System for Security Threat Assessment." Proceedings of Second Annual Symposium on Physical/Electronic Security. August 1986. This article describes a risk

analysis methodology called ATAM developed by Arthur D. Little Inc. The methodology provides coverage of such issues as: physical property damage; information disclosure; information modification; loss of data integrity; and interruption or denial of service.

Jacobson, Robert, V. "Organizing and Conducting an Automated Risk Analysis." DOE 7th Computer Security Group Conference. April 10-12, 1984. New Orleans, Louisiana. This paper considers the most important advantages of automation, and shows how a computer security manager can use them effectively. The article specifically focuses on the use of RAMP, IST's risk analysis software package.

Jensen, Tom. "Navy Automates ADP Risk Assessment Procedures." Government Computer News. April 29, 1988. p. 51. This article describes a risk analysis tool called REACT developed by Tidewater Consultants, Inc. to be used at the Naval Aviation Logistics Command Management Information System (NALCOMIS).

Mayerfeld, Harold and Troy, Gene. Center for Computer Security News. Vol. 7. No. 1. July 1988. This article describes the concept for an expert system called the M2Rx (Martin Marietta Risk Expert) for use in performing knowledge-based risk management.

Moses, Robin H. and Clark, Rodney. "The CCTA Risk Analysis and Management Methodology: CRAMM." Proceedings of 10th National Computer Security Conference. 21-24 September, 1987. This article describes a risk analysis methodology called CRAMM that was developed in Great Britain. It was developed to meet thirteen mandatory requirements.

Smith, S.T. and Phillips, J.R. "Assessing the Threat Component for the LAVA Risk Management Methodology." DOE 9th Computer Security Group Conference. This paper discusses problems of assessing threats using the LAVA methodology.

White, Gregory B. "ATAM: A PC-Based Air Force Risk Analysis Tool." 10th DOE Computer Security Group Conference. 5-7 May, 1987. Albuquerque, New Mexico. This article describes a risk assessment methodology called ATAM that was developed for the USAF by Arthur D. Little Inc. It uses a series of digraphs to model events associated with the security of a computer system.

THREATS AND VULNERABILITIES

Aaron, Diana B. and Green, Lee. "Today's Computer Crime: The Threat from Within." Information Week. October 26, 1987. pgs. 34-45. This article describes a variety of current threats to computer systems, and discusses simple countermeasures available in physical security, access control, transmission security, and encryption/decryption to counter these threats.

Baker, Lara H. "Threats to DOE Computers: A Perspective." DOE 11th Computer Security Group Conference. May 3-5, 1988. This paper discusses the difference between threats from insiders, threats from outsiders, and vulnerability-induced-threats.

Bequai, August. "Computer Snafus Keep Government in High-Tech Dark Ages." Government Computer News. June 20, 1988. pp. 52-53. This article describes

several computer fraud incidents that affected the Federal Government during the last several years.

Campbell, Douglas. "Computer Site: Targets for Destruction." Security Management. July 1988. pp. 57-60. This article gives recent real-life examples of terrorist attacks against computer centers worldwide. It explains that terrorism generally requires symbols, and, as a result, conspicuous computer sites often become targets for bombings and other means of physical destruction.

Courtney, Robert H., Jr. "Protection for Sensitive and Other Valuable Data." Center for Computer Security News. Vol. 7., No. 1, July 1988. This article discusses the important differences between the threat of disclosure of sensitive data vs. the threats of fraud, embezzlement, tampering, and misuse of data. The article strongly recommends sensible security approaches that take all threats to our data into consideration.

Hafner, Katherine M. "Is Your Computer Secure." Business Week. August 1, 1988. pp. 64-72.

Moulton, Rolf T. "Dealing with System Abuse: Steps to Take When Victimized." 1986 Datapro. August 1986. This report provides a comprehensive discussion of the various types of abuse techniques currently being used to attack computer systems, and the steps that a victim should follow to cope with and protect against such attacks.

Musacchio, John and Rozen, Arnon. "Computer Sites: Assessing the Threat." Security Management. July 1988. pp. 41-51. This article examines computer center vulnerabilities in a historical and international context, and describes a realistic terrorist threat scenario against a computer center. The primary focus is on threats that impact the physical structure and viability of the center and countermeasures available to offset them.

Parker, Donn B. "Computer Crime Methods." 1985 Datapro. IS09-200-101. May 1985. This article provides a detailed review of the myriad threats that can affect a computer system, to include realistic examples of how these threats affect a system. Countermeasures for each threat described are also presented.

Thackeray, Gail. "Computer Security: The Menace Is from Inside." The Office. October 1988.

Whitehurst, Susan A. ed. "How Business Battles Computer Crime." Security. October 1986. This article shows how valuable computers are to business and how vulnerable they are to crime. The article presents new statistics on these subject areas based on the results of the 1986 Computer Crime Survey conducted by Security.

Zalud, Bill. "Security and DP Corporate to Attach Computer Crime." Security. October 1987. pp. 52-58. This study was conducted to determine the security decision makers' awareness and actions regarding loss of information, assets, financial resources and productivity as a result of tampering with computer-based information and/or theft of or damage to computers.

"The Vulnerabilities of Communications Systems." Datapro. IS35-120-101,

October 1987. This report focuses on malicious or deliberate unauthorized access and alteration, principally because it is in these areas that the impact of Federal policies is greatest.

COUNTERMEASURES: EQUIPMENT AND TECHNOLOGIES

"All About Microcomputer Encryption and Access Control." 1987 Datapro. IS31-001-112. July 1987.

"An Overview of Physical Security Devices for Microcomputers." 1988 Datapro. IS33-001-101. February 1988

Clark, Clara I., and Miller, Steven S. "METC's Software for the Protection of Unclassified Sensitive Information." Proceedings of Second Annual Symposium on Physical/Electronic Security. August 1986. This paper describes vulnerabilities inherent in commonly used security software (or software that provide security functions) based on five pieces of software contributed voluntarily to the DOE's Morgantown Energy Technology Center's computer security program. The paper illustrates the effectiveness of human controls against threats to computer systems, and emphasizes that technical safeguards alone are virtually ineffective in counteracting inappropriate activities on the computer.

Cyphers, Clifford K. "Selecting the Right Wire and Cable for Security." Data Processing and Communications Security. Summer 1988. This article provides a simple wire and cable checklist for use in identifying the right cabling for your communications/computer security needs.

Jackson, Carl. "Clean up Your Electricity Act." Security. March 1988, pp. 34, 36. This article describes the danger of electrical disruptions and the need to protect mainframe and microcomputers. Various protection approaches are discussed, including: UPS; back-up generators; power line surge protection; and anti-static protection.

Jones, Mitt. ed. "You Can Take It with You." PC Magazine. September 13, 1988. This article describes the advantages and shortcomings of removable hard disks, flexible cartridge systems, and removable hard cartridges.

Lydon, Kerry. "Halon Adds To Fire Safety of High Value, High Risk Materials and Equipment",-- Equipment Focus." Security. May 1988, pp. 52-56 This article describes the advantages of Halon fire suppression systems and types of Halon suppression systems: pre-engineered or modular.

Manro, Neio. "Tempest Security Industry Braces for Tough Times." Defense News. April 17, 1989. This article describes that national policy required that all computerized classified information be stored on TEMPEST computers.

Naudts, John. "Access Control Market Gives Clients Many Options." Government Computer News. February 13, 1987. pp. 40-41. This article provides an overview of the various access control products currently available that can be considered for use in the computer world. It also addresses issues to consider for future planning of access control needs.

1988 Computer Security Buyers Guide. Computer Security Institute. 1988. This handbook provides a listing of various security products and suppliers for use in identifying appropriate computer security countermeasures.

Security 1988 Forecast Study. Security's Marketing Research Affiliate. Des Plaines, IL. October 1987. The primary objective of this study is to identify the future direction of security equipment applications and technology from a questionnaire mailed to security decision makers in industry.

Steinauer, Dennis. "Securing Your PC Which Security Devices Should You Select." Security, September/October 1986. This article provides a careful discussion of the many issues associated with identifying and selecting devices for security the computer environment. It covers access control products, electrical power quality products, magnetic media protection, the use of security bulletin boards (to include NIST's), encryption and communications security. It also provides guidance on developing your own individualized action plan for selecting devices appropriate for your environment.

Troy, Eugene F. "Hardware Protection of Communications Ports and Lines." Data Security Management. 84-03-20 1986 Auerbach Publishers Inc.

COUNTERMEASURES: PROCEDURES

Conca, Edward W. "Agencies Can Use Checklist To Begin Security Plan." Government Computer News. June 20, 1986, p. 60. This article provides a framework for implementing and maintaining an all-inclusive computer security program.

Cronin, Daniel J. Microcomputer Data Security Issues and Strategies. A Brady Book. Prentice Hall Press. New York. 1986. This handbook for computer users provides a description of security procedures for the PC environment, including discussion of log-on approaches, access guards, and the secure use of modems for network security.

Feinstein, Hal. "Security on Unclassified Sensitive Computer Systems." Proceedings of 9th National Computer Security Conference. 15-18 September, 1986. This paper deals with some of the security issues facing unclassified sensitive computer systems that are operated by the civil agencies of the Federal Government, and describes various measures available to offset these problems.

Gerberick, Dahl A. "A Checklist for Security and Contingency Planning." Data Security Management. 1986 Auerbach Publishers Inc. 82-01-10. This article provides a thorough review of all critical areas that should be considered in planning the security and contingency operations of a computer center or system.

Isaacson, Gerald L. "Programmer Workstation Security." Data Security Management. 84-05-30. 1986 Auerbach Publishers Inc. This article discusses the various strategies for protecting information from the risk of exposure at the workstation level.

Karabin, Steven. "Data Classification: Getting Started." Computer Security

Newsletter. May/June 1986. This article briefly describes the considerations one must make in reviewing data bases to determine the appropriate level of classification as a first step in securing your database.

Llana, Jr., Andres. "Disaster Recovery Planning an Integrated Network Environment." Datapro. IS35-220-101. March 1989. This report discusses the various elements that are involved that are involved and should be considered in the disaster recovery process. The model for this discussion focuses on a typical business situation involving multiple locations and an integrated network environment.

Page, Marcus. "Passwords Are Still Best Security Method." Government Computer News. July 19, 1988. This article discusses the pros and cons of using passwords, emphasizing that the pros outweigh the cons.

Parker, Donn B. "Safeguards Selection Principles." Computers & Security. May 1984. Vol.3. No. 2. This article presents 20 principles that are practical for everyday use in the performance of computer security reviews and EDP operational audits.

Parker, Donn B., Johnson, Robert M., and others. Computer Security Techniques. National Criminal Justice Reference. P.O. Box 6000, Rockville, MD.

Shaw, Dennis F. Computer Security A Review of Some Problems and Possible Solutions. 1986 International Carnahan Conference on Security Technology. Gothenburg, Sweden. August 12-14, 1986. This review includes a survey of various security techniques currently in use to secure computers. Software, hardware and personnel procedures are addressed.

Whieldon, Althea M. "Passphrase Management System." Proceedings of Second Annual Symposium on Physical/Electronic Security. August 1986. This article describes the DoD Password Management Guideline developed by the National Computer Security Center (NCSC).

Withrow, Janet B. Security Handbook for Small Computer Users. Air Command and Staff College. Maxwell AFB, AL. April 1985. 3-1 3-5

Zalud, Bill. "When Computers Talk, Too Many Listen." Security. January 1988. This article describes the problems associated with access to on-line computers. A description is provided of selected specific problems along with suggestions for actions to offset them.

NETWORKS

"All About Securing Micro-to-Mainframe/Minicomputer Links." 1987 Datapro. IS34-001-101. August 1987.

Branstad, Dennis K. "Considerations for Security in the OSI Architecture." 84-07-30. Data Security Management. 1986 Auerbach Publishers Inc.

Callis, Melinda and Skolnik, Sheryl. "Establishing the Microcomputer-Mainframe Link." Data Security Management. 84-04-19 1986 Auerbach Publishers Inc.

Cotnoir, Marc. "Security Local Area Networks." 1986 Datapro. IS35-150-101. January 1986.

Crutcher, Richard I. and Ewing, Paul D. "A Mixed-Modem Solution for Sensitive Data Segregation on a Broadband Network." 11th DOE Computer Security Group Conference. May 3-5, 1988. Kansas City, Missouri.

Highland, Harold. "A Secure Network Must Be an Unfriendly Network." Government Computer News. October 10, 1988.

Kent, Stephen T. and Tauss, Gary. "As Networks Proliferate, So Should Security Plans." Government Computer News. June 20, 1986. pp. 39, 66-67.

"Limitations of Dial-up Security Devices." 1986 Datapro. National Bureau of Standard's Institute. IS35-320-101. November 1986.

Mehrmann, Louis, W. "Good Security Practices for Information Systems Networks." DOE 9th Computer Security Group Conference. May 6-8, 1986, Las Vegas, Nevada.

Pierson, L.G. and Witzke, E.L. "Elements of a Proposed Security Methodology for Networks of Computers." 10th DOE Computer Security Group Conference. 5-7 May, 1987. Albuquerque, New Mexico.

Reel, Nanci. "Data Security in Local Area Networks." Data Security Management. 84-04-23 1986 Auerbach Publishers Inc.

Sobol, Michael I. "Security Concerns in a Local Area Network Environment." Telecommunications. March, 1988. pg. 96-100. This article addresses the security and control measures of a LAN environment that prudent businesses will want to implement and security administrators will need to review.

Stoll, Cliff. "To Catch a Hacker: Traceback Techniques." 1988 Datapro. IS35-290-101. May 1988.

Troy, Eugene F. Security for Dial-Up Lines. NBS Special Publication 500-137. May 1986.

Wiedemann, Peter H. "Separation Techniques Offer Data Security Options." Government Computer News. July 17, 1987. p. 74.

VIRUS AND OTHER RELATED THREATS

"A Manager's Guide to Computer Viruses." Computer Security Institute. This handbook provides a basic knowledge for managers involved with data processing to understand what a computer virus is, what it does, how to detect the presence of a virus, and how to defend against it.

Bologna, J., ed. Computer Security Digest. August 1988. Vol VI, No. 5. This digest covers how computer viruses beginning to "Bug" top management people, disasters occurred recently, and computer viruses protection: Disk Watcher V: 2.0.

Bologna, J., ed. Computer Security Digest. December 1988, Vol VI, No. 9. This digest covers several issues including virus scare, management's concerns, virus vaccines, disaster recovery, and late news about viruses.

DiDio, Laura, (ed.). "Caution: Viruses at Play." Network World. July 4, 1988. pgs. 29, 30, 33, 34. This article reviews the several virus incidents occurred in U.S. firms recently and describes some precautionary measures that users can adopt to minimize the risk of infection.

DeWitt, Phillip E. "Invasion of the Data Snatchers." Time. September 21, 1988. pgs. 62-67. This article describes incidents caused by viruses over the past years and information on software to detect viruses along with anti-virus programs. Some specific examples are given with regard to actual instances of computer virus attacks.

Glath, Raymond M. Computer Viruses: A Rational View. RG Software Systems, Inc. April 14, 1988. This article represents general view of computer viruses, including two major categories of viruses (destructive viruses and non-destructive viruses), threat, protection, and virus protection packages.

"Hardware Virus Threatens Databases." Advanced Military Computing. December 5, 1988. Vol. 4, No. 25. This article describes that the chips called Intel 8272A and the NEC 765 made by Intel Corp. and NEC Electronic Inc. can corrupt data in disk drives.

Hilts, Philip J. "Virus Hits Vast Computer Network." The Washington Post. November 4, 5, and 7, 1988. This article describes the virus incident which hit vast computer networks by a Cornell Graduate student, affecting Internet links as many as 50,000 computers.

Jackson, Carl. "What Is a Computer Virus." Security. May 1988, pgs. 24, 26

Magid, Lawrence J. "There Are Ways to Protect Your Personal Computer from 'Viruses'." Washington Post. November 20, 1988. This article discusses ways to protect personal computers from 'viruses' through backuping up your data on a regular basis and avoiding the exchange of programs with others.

Nomani, Asra, Q. "Bug Busters Devise Electronic Vaccines for Computer Viruses." Wall Street Journal. June 17, 1988. This article discusses electronic vaccines for computer viruses.

Pozzo, Maria M. and Terrence, Gray. "Managing Exposure to Potentially Malicious Programs." Proceedings of 9th National Computer Security Conference. 15-18 September, 1986. This article describes various approaches for use in reducing your risk to harmful programs; the approaches include: limited sharing, dynamic auditing, detection of modified programs, and decreasing your exposure to high-risk software.

Rivera, Angel. "Computer Viruses Can Infect Entire Organizations." Government Computer News. April 29, 1988.

Rivera, Angel L. "The Year of the Virus." Data Processing & Communications Security. Summer 1988. Vol. 12, No. 3. This article describes four basic

types of malicious software that can harm a computer and its operations, including: logic bomb; worm program; trapdoor; and Trojan horse. The article also describes several new approaches to detecting software modifications taken by Digital Dispatch Inc. (DDI).

"Some Viruses 'Bomb' Hardware." Advanced Military Computing. January 16, 1989. Vol. 5, No. 2. This article describes how to protect hardware from selected types of viruses which can destroy hard disk drives.

Vogel, Shawna. "Disease of the Year: Illness as Glitch." Discover. January 1989. This article reviews the major virus attacks to U.S. computers during the last several years and also provides a brief review of countermeasures available to detect viruses.

Young, Catherine L. "Taxonomy of Computer Virus Defense Mechanisms." NBS/NCSC 10th National Computer Security Conference. 21-24 September, 1987. This important article reviews six schemes for detecting and defending against computer viruses, and provides detailed discussion of each approach and its elements.

RISK MANAGEMENT

"American Computer Security Management Guide." American Computer Security. 1986. This guideline describes approaches useful in justifying security to those controlling the budget. Sample policies and procedures are also provided as useful formats for adoption by an organization just starting out.

Beall, Thomas, Bowers, Robert A., and Lange, Andrea G. "Stacking the Odds in Your Favor." Security Management. August 1982. pp. 57-65. This article is intended to guide public and private security managers as they conduct vulnerability and risk assessments for internal control. Several models for these analyses are discussed, and the strengths and weaknesses of the various approaches are highlighted.

Berlonghi, Alexander and Mattman, Jurg. "New Trends in Risk Management: Opportunities for Excellence." 1986 Datapro. IS20-320-101. July 1987.

Moses, Robin H. "Risk Analysis and Management in Practice for the U.K. Government." NBS/NCSC 10th National Computer Security Conference. 21-24 September, 1987.

Proceedings of 1988 Computer Security Risk Management Model Builders Workshop. May 24-26, 1988. Denver, Colorado. Sponsored by Martin Marietta, National Bureau of Standards, and National Computer Security Center.

Roberts, Martin B. EDP Controls 1985. John Wiley & Sons, N.Y. This handbook sets forth a general program for EDP controls and contingency planning.

Schabeck, Tim A. "Risk Management Policy: Planning for the Day When It Doesn't Happen to the Other Guy." Computerworld. April 30, 1984. p 34. This article describes important controls that should be in place in the computer environment to effectively manage risk. These controls include establishing policies and procedures that govern equipment inventory and access, along with

control of the applications being processed.

Schweitzer, James, A. "A Management View: Computer Security as a Discretionary Decision." Computer & Security. 1985. pp. 13-22. This article discusses computer security as a key facet in an overall business information resource management environment.

Thompkins, Fred. "Information Security Risk Management." 1986 Datapro. IS20-160-101. May 1986.

CERTIFICATION AND ACCREDITATION

Ferris, Martin and Cerulli, Andrea. "Certification: A Risky Business." 10th NBS/NCSC National Computer Security Conference. 21-24 September, 1987. This paper addresses certification in management terms, provides examples of certification in everyday life, and examines ways to maximize the use of national resources and policies to achieve a certified AIS application.

Stevens, Jennie; Barbour, James; and Moradi, Debbie. "Managing the Accreditation Process: Lessons Learned." Proceedings of Third Annual Symposium on Physical/Electrical Security. August 1987. This article describes the process of computer system accreditation, the key steps involved in accreditation, and the critical management considerations that must be factored into the process to ensure its success. The article was developed based on hands-on experience from past accreditation experiences of the authors.

OTHER U.S. GOVERNMENT COMPUTER SECURITY PUBLICATIONS

Department of Agriculture. ADP Security Manual. DM3140-1. July 19, 1984.

Department of the Army. Automation Security. 13 March 1987.

Department of Commerce. National Bureau of Standards. (Branstad, Dennis K. and Reed, Susan K.) Executive Guide to Computer Security. Department of Commerce. National Bureau of Standards. Computer Security Publications. NBS List 91. July 1988.

Department of Defense. Security Requirements for Automated Information Systems (AISs). No. 5200.28. March 21, 1988.

Department of Defense. National Computer Security Center. Various Publications (to include the Orange, Yellow, and Red Books.)

Department of State. System Security Standards. (Number 1 Number 5). 1985.

Department of Treasury. Handbook for Automated Information Systems Security and Risk Management. TD 85-02. April 1987.

General Services Administration. Automated Information Systems Security. IRM P 2100.5. October 26, 1987.

U.S. Postal Service. ADP Security Handbook AS-805. Washington, D.C. 20260-1511. August 1, 1988.



NIST-114A
(REV. 3-90)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER	NISTIR 4325
2. PERFORMING ORGANIZATION REPORT NUMBER	
3. PUBLICATION DATE	MAY 1990

4. TITLE AND SUBTITLE
 U. S. Department of Energy Risk Assessment Methodology
 Volume I: DOE Risk Assessment Guideline Instructions, Resource Table, and Completed Sample
 Volume II: DOE Risk Assessment Worksheets

5. AUTHOR(S)
 Edward Roback, NIST Coordinator

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)
 U.S. DEPARTMENT OF COMMERCE
 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
 GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

 8. TYPE OF REPORT AND PERIOD COVERED
 NISTIR

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)
 Reprinted by permission of the U.S. Department of Energy, Office of ADP Management and the
 Computer and Technical Security Branch, Washington, DC 20545

10. SUPPLEMENTARY NOTES

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

This publication reprints two volumes of a risk assessment guideline developed by the Department of Energy. Volume I: The DOE Risk Assessment Instructions, Resource Tables, and Completed Sample -- A Structured Approach and Volume II: DOE Risk Assessment Worksheets are the result of a joint program sponsored by the Department of Energy's (DOE) Office of ADP Management and the Computer and Technical Security Branch. It was developed for DOE under contract by Booz, Allen & Hamilton, Inc. The guideline was developed to allow ADP Managers and end users to quickly understand and accomplish risk assessments in a more effective and expeditious fashion.

The Guideline is organized into two separate volumes. (Both Volume I and II are included in this publication.) Volume I, the main body of the Guideline includes general instructions and references. Volume I also consists of instructions for Steps 1 through 6. Also, included are a glossary and bibliography, which follow Volume II. Volume II consists of the worksheets for each step for completing the Guideline.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)
 accreditation; ADP security; automated information system security; certification; computer security; countermeasures; risk assessment; risk management; viruses; vulnerability assessment

13. AVAILABILITY

<input checked="" type="checkbox"/>	UNLIMITED
<input type="checkbox"/>	FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).
<input type="checkbox"/>	ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.
<input checked="" type="checkbox"/>	ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES	194
15. PRICE	A09

ELECTRONIC FORM



