

NIST
PUBLICATIONS

U.S. DEPARTMENT OF COMMERCE

METHODOLOGY FOR CERTIFYING SENSITIVE COMPUTER APPLICATIONS

**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**

QC

100
.U56
#4451
1990
C.2

NIST

NATIONAL INSTITUTE OF STANDARDS &
TECHNOLOGY
Research Information Center
Gaithersburg, MD 20899

11120-1

U.S. DEPARTMENT OF COMMERCE

METHODOLOGY FOR CERTIFYING SENSITIVE COMPUTER APPLICATIONS

**Edward Roback
NIST Coordinator**

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

November 1990



**U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
John W. Lyons, Director**

FOREWARD

This National Institute of Standards and Technology Interagency Report (NISTIR) presents the Methodology for Certifying Sensitive Computer Applications developed by the U.S. Department of Commerce, Office of Information Resources Management.

The National Institute of Standards and Technology (NIST) makes no claim or endorsement of this certification 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 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 Commerce for their kind 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.

U.S. DEPARTMENT OF COMMERCE

**METHODOLOGY FOR CERTIFYING
SENSITIVE COMPUTER
APPLICATIONS**

**U.S. DEPARTMENT OF COMMERCE
METHODOLOGY FOR CERTIFYING
SENSITIVE COMPUTER APPLICATIONS**

PREFACE

Appendix III to OMB Circular No. A-130 establishes a minimum set of controls to be included in Federal automated information systems security programs. It specifies that, at a minimum, the program will include four primary elements: application security, personnel security, information technology installation security, and security awareness and training. This document addresses only one of those primary elements: application security, and more specifically, the management control process as described in the Appendix.

The application security "management control process" includes three main elements: 1) developing security specifications which are intended to assure that appropriate administrative, physical, and technical safeguards are incorporated into (or surround) the application; 2) design reviews and systems tests intended to prove the existence and adequacy of the security safeguards, and; 3) certification that the application meets all applicable Federal policies, regulations, and standards, and that the results of the system tests demonstrate that the installed security safeguards are adequate for the sensitivity of the application. Although not specifically stated in the Appendix, discussions with the OMB revealed that achieving and maintaining accuracy of data is also a security objective to be accommodated.

The management control process elements are application-specific. Although some of the security safeguards may be common to other applications, the determination of security requirements, and the subsequent system tests will be different for each application. This means that there are no real shortcuts to achieve certification, such as checklists or similar approaches. Such approaches, although invitingly simple and inexpensive to administer, cannot achieve the individuality required for each application. Rather, they may lead the user to over-protect, under-protect, or completely over-look vulnerabilities of the application.

This document prescribes a methodology which, if applied diligently, addresses the individual security needs of each application and assures full compliance with OMB application security requirements. Further, it enables the certifying official to have reasonable confidence in the fact that appropriate security measures are in place and are adequate for the sensitivity of the application being certified.

Finally, it should be noted that this methodology does not describe the specific security criteria for each application. These must be developed on an application-by-application basis and will determine the scope and complexity of each certification project. For example, a relatively minor PC-based application may require nothing more than backup and security for the "floppy" disks or the PC. The documentation for such an application could denote the reason for and degree of sensitivity, security requirements, safeguard provided (i.e. formal procedures), and satisfaction that the procedures are being followed ("systems test"). Obviously, highly sensitive and complex applications will represent the other extreme, requiring more documented controls and safeguards which must be installed and tested to the satisfaction of the certifying official. The important point is that the methodology should be followed, if only mentally, to ensure that each step is consciously considered and that the rationale for the actions taken or not taken will satisfy the certifying official, whoever that may be.

**U.S. DEPARTMENT OF COMMERCE
METHODOLOGY FOR CERTIFYING
SENSITIVE COMPUTER APPLICATIONS**

TABLE OF CONTENTS

	<i>page</i>
I. Purpose	1
II. Scope	1
III. Definitions	1
IV. General	2
A. Certification Concept	2
B. Documentation	3
C. Project Staffing	7
V. Methodology for Certifying Computer Applications	9
VI. Recertifying a Sensitive Application	41

FIGURES

IV-1 Standard Worksheets	5
V-1 Overview of Sensitive Application Certification	11
VI-1 Overview of Sensitive Application Recertification	43

ATTACHMENTS

- A Description of Sample Worksheets
- B Examples of Certification/Recertification Statements
- C Examples of Certification Documentation

U.S. DEPARTMENT OF COMMERCE
METHODOLOGY FOR CERTIFYING
SENSITIVE COMPUTER APPLICATIONS

I. PURPOSE

To define and describe a standard certification methodology for the Department of Commerce: (a) to ensure that sensitive applications meet applicable Federal policies, regulations, and standards, and (b) to demonstrate that the installed security safeguards are adequate for the sensitivity or criticality of the data processed, as required by OMB Circular A-130.

II. SCOPE

Certification is required for all computer applications within the Department which are determined to be sensitive within the context of OMB Circular A-130. The management control process leading to certification, as prescribed in the circular, will be incorporated early in the developmental process of new applications or when substantial changes are to be made to existing applications. The circular also requires recertification of existing applications at least every three years. This recertification requirement implicitly directs an initial certification for each sensitive application.

III. DEFINITIONS

For the purposes of this methodology, the following definitions will apply:

Certification: A process culminating in a statement signed by a Department of Commerce official certifying that the application satisfies all appropriate Federal policies, regulations, and standards, and that the results of tests demonstrate that the installed security safeguards are adequate for the sensitivity of the data handled by the application.

Certifying Official: A senior DOC official, such as the Senior Official for Information Resources Management, who has the authority to accept or reject the security safeguards of an application and issue the certificate recording the decision. The official must possess the authority to direct that security deficiencies be remedied, and to allocate appropriate resources to achieve acceptable security.

Critical Application: A computerized application which may or may not be sensitive as defined by statute, regulation, or Departmental policy, but which is essential to the successful performance of a major Departmental mission. These critical applications are considered to be sensitive within the scope of OMB Circular A-130 because of the risk and magnitude of loss or harm that could result from improper manipulation or the inability to process.

Evidential Requirement: The specific responses or reactions which must be evidenced by a security feature to prove that the feature is present, performs as specified, and satisfies the intended functional security requirement(s) stated by the user. Also used herein as "Required Evidence of Adequacy".

Functional Security Requirement: A Security-related requirement expressed by the user(s) in their own terms, indicating specific restrictions, authorizations, edits, privileges, accesses, reasonableness tests, ranges, processes, results, and other requirements necessary to assure adequate security, accuracy, and availability of the application and its data. These requirements, although stated in functional terms, must be specific and measurable to the extent that they can be translated into technical, procedural, or administrative controls or safeguards.

Information Technology Facility: An organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology.

Security Features: The systemic controls or safeguards which can be in almost any form including manual or automated, physical or logical, procedural, or otherwise, and which are specifically designed or

prepared and implemented to provide the degree of protection specified by one or more functional security requirement. A security feature may be implemented in the application, the facility, communications, user areas, or any other appropriate location.

Security Feature Specifications: A detailed description of each security feature required to protect a sensitive application. The specifications should include: (a) a description of the safeguards necessary to ensure the protection, accuracy and integrity of the sensitive application and associated data, (b) how they will function and what they will do, (c) how and where they will be implemented, and (d) how they will satisfy one or more of the functional security requirements.

Sensitive Application: An application of information technology requiring protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from its loss, or improper, access, operation, or manipulation of the application and its data, whether intentional or unintentional.

System: The organized collection, processing, transmission, and dissemination of information in accordance with defined automated and/or manual procedures, and including the environment and resources required for its successful operation. Any use of the word "system" within this document will be within the totality of this definition.

Test Scenario(s): A detailed series of actions, manual and/or automated, which are designed to prove or disprove (produce the evidential requirements) that the security features being examined in this scenario are performing as intended and required, and are providing the degree of protection appropriate to the sensitivity of the application.

User(s): An organizational or programmatic entity that receives service from an information technology facility. A user may be either internal or external to the DOC organization responsible for the facility, but normally does not report either to the manager or director of the facility or to the same immediate supervisor.

IV. GENERAL

Under ideal circumstances, security requirements should be specified prior to the beginning of application development so that they can be incorporated into the developmental process along with other functional processing requirements. Such an approach not only provides better assurance of security but does so with less problems and costs than a later retrofit of security features. This methodology will not attempt to describe the developmental process, of which there are many variations, but will address security related aspects which can be, and should be incorporated into any developmental methodology.

There are many variations of sensitive applications with no two being exactly alike. A certification methodology must be adaptable to these variations. Accordingly, this methodology should be used as a guide, and is not intended to replace professional judgement and intimate knowledge of the operating environment, function supported, or application.

(NOTE: If a risk analysis has not been performed at the installation, the cost to secure each sensitive application will probably be substantially higher. Because of this, it is highly recommended that an installation risk analysis be performed prior to the start of application certification).

A. Certification Concept

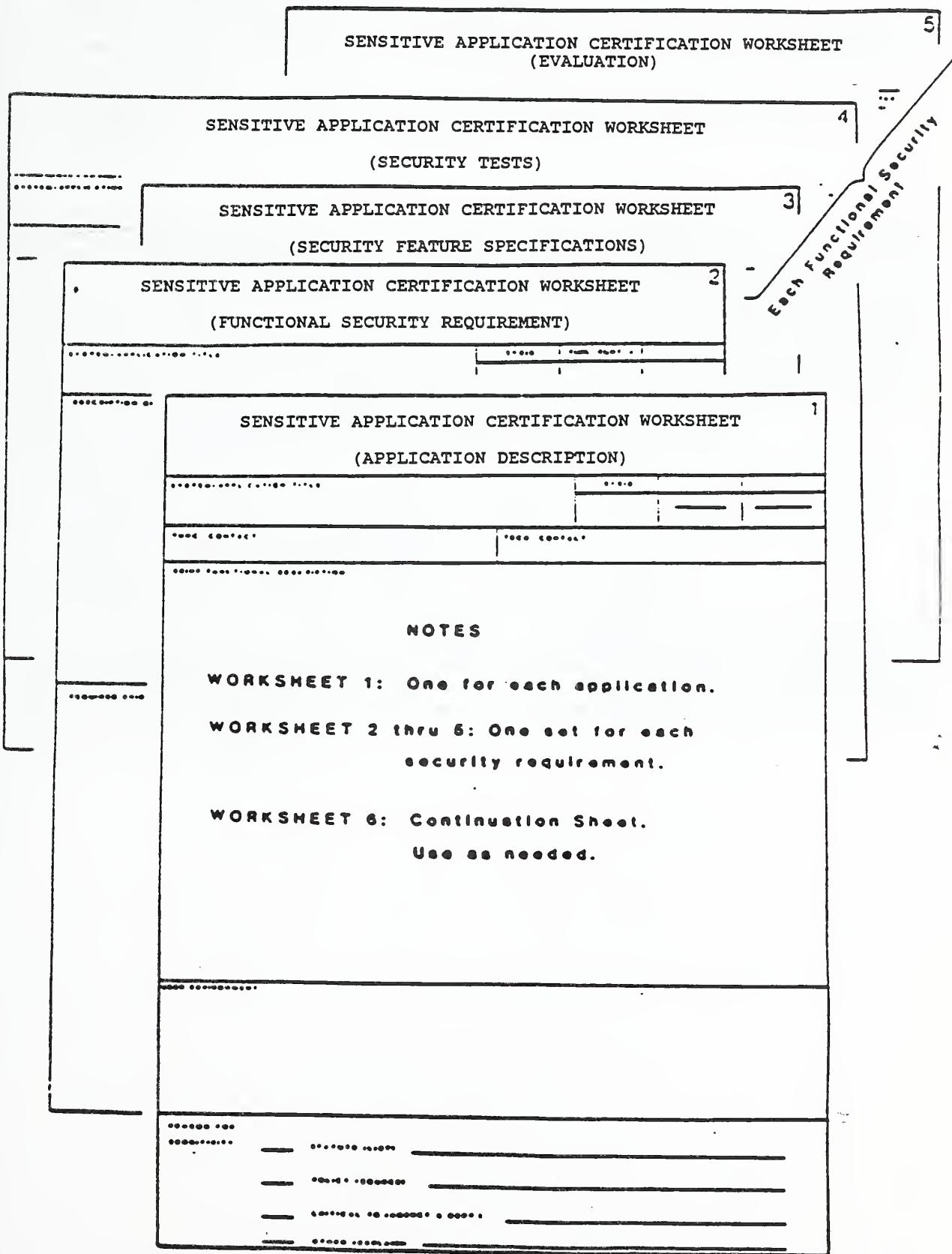
1. Identify sensitive applications. Application sensitivity must be determined by the users in view of their knowledge of the sensitivity and criticality of the application. If there are more than one sensitive application within a user element, that element should arrange their applications in order of their sensitivity or importance to the user. If more than one user is involved, all of the sensitive applications must be merged and arranged in a single order of priority for certification. The assignment of priorities must be made at a sufficiently high level of management where objectivity can be assured and the priorities of DOC will prevail over those of individual users. Finally, a cut-off level must be established, above which all applications must be certified while those below the level may be considered as acceptable risks and therefore non sensitive. The certification or recertification of sensitive applications should then start with the highest priorities.

2. Determine security needs. The data owner or users must articulate the security requirements for the application if this has not already been done. These requirements, although stated in functional terms, must be specific and measurable to the extent that they can be translated by others into technical, procedural, or administrative controls or safeguards. In addition to the security requirements specified by statute, regulations or policy, other external inputs such as IG and audit reports must be considered.
3. Design, review and approve safeguards. Security safeguards can embody many forms such as the formulation of additional or revised policies and procedures, physical measures, computer software, comprehensive edit checks, access control system, or a myriad of other possibilities. Appropriate and cost-effective safeguards must be devised to satisfy each of the approved functional security requirements. The responsible person or organization designated to design and prepare the specifications for the safeguard or control will depend upon its nature, the type of skills required, and where it is to be employed. After all have been designed, they must be evaluated by a panel of experts to assess their individual and collective capability to provide the degree of protection appropriate for the sensitive application.
4. Test safeguards. After approval, preparation, and installation, safeguards must be tested to ensure that they are in place and are operationally adequate. Specific test scenarios must be designed and executed, and the results analyzed to ensure that the adequacy of each feature has been proven. Features producing unsatisfactory results must be revised and retested, or the user management must opt to accept the risk of not having the feature. Following this, an evaluation report will be prepared for the certifying official.
5. Certify the application. The Certifying Official will review the security evaluation report to determine if the tests demonstrate that the installed security safeguards are adequate for the sensitivity of the data handled by the application. The Certifying Official may unconditionally certify the application; certify with conditions or restrictions; or withhold certification until certain changes or corrections are made.

B. Documentation

1. The decision of the Certifying Official will be primarily based upon an evaluation report summarizing the detailed documents developed during the evaluation and certifying process. OMB Circular A-130 requires this full documentation and directs that it be maintained in the official DOC agency records since they will have a continuing value to the organization. They will be particularly valuable to the ADP security staff, auditors and inspectors general, to serve as the starting point for subsequent recertification of the application, and as input to the periodic facility risk analysis.
2. Since each application to be certified will present different situations and problems, it is most important that these be documented in a standard manner which will stand the test of time and changing personnel. This methodology includes suggested formats for worksheets to be used to document the evaluation and certification process. The use of these worksheets is not mandatory. Examples of these worksheets and instructions for their use are contained at Attachment A. This attachment also describes the entries required on each worksheet. Attachment C contains an example of the worksheets completed for a fictitious sensitive application.
3. Figure IV-1 shows the relationship of these worksheets. Detailed instructions for their use to certify or recertify applications are contained in Sections V and VI, respectively. The worksheets are intended to be used as follows:
 - a. Worksheet 1, Application Description, is intended to generally describe the application and the reasons why it is considered to be sensitive. One will be prepared for each potentially sensitive application to be evaluated.
 - b. Worksheet 2, Functional Security Requirement, is used to describe each security-related requirement needed to provide an acceptable level of protection for the application. Unless requirements are very closely related, each will be described on a separate Worksheet 2.
 - c. For each security requirement (Worksheet 2), there will be a corresponding Worksheet 3, Security Feature Specifications. This is used to describe the proposed security control or safeguard, including detailed specifications if appropriate.

Figure IV-1: STANDARD WORKSHEETS



- d. For each Security Feature Specifications (Worksheet 3), there will be one or more planned security tests designed to prove the presence and effectiveness of the security feature. These tests will be documented on Worksheet 4, Security Tests. When the tests are executed, the results of these tests will also be recorded on Worksheet 4.
- e. For each security test documented on Worksheet 4, there will be a corresponding analysis and evaluation of the results of each test, with appropriate recommendations, to be summarized on Worksheet 5.
- f. Worksheet 6 is a continuation sheet which may be used to extend any portion of the other Worksheets.

C. Project Staffing

- 1. In a certification or recertification project only three staffing requirements are certain—the certifying official, an application certification manager, and one or more application users. There will be a need for others, but the specific skills and numbers required will vary widely from application to application, and from time to time during the project. The Application Certification Manager will be the person to make these decisions and to arrange for, and receive, assistance when needed. Whether from a user organization or from a technical support organization (e.g. ADP), the Application Certification Manager must be given authority commensurate with the responsibilities which have been assigned. Without this clearly defined authority, the project should not be undertaken since it will surely fail. (As used here, Application Certification is synonymous with Application Recertification). The Application Certification Manager should be charged with:
 - a. Initiating the project.
 - b. Arranging for internal and external security evaluation support resources, scheduling their participation to coincide with the needs of the project.
 - c. Managing the security evaluation to completion.
 - d. Preparing the security evaluation report(s), with assistance, if needed.
 - e. Providing periodic status reports to management.
- 2. Other skills which may be required at various times include auditors, inspectors general, users, industrial security staff, various data processing skills, facilities engineer, communications, and others. The Application Certification Manager must determine the skills and numbers needed, and when they will be required based upon the nature of the application to be evaluated and certified and the progress of the project.

V. METHODOLOGY FOR CERTIFYING COMPUTER APPLICATIONS

Figure V-1 is a graphic representation of the process leading to certification of a computerized application. Each block in the figure will be described in sufficient detail to allow the reader to understand the process and to adapt it to any application. The number above each block corresponds to the following paragraph number. When needed to describe particularly lengthy or complex tasks, sub-tasks will be described and similarly identified in the text. Worksheets specifically designed to document the security evaluation and certification process are included in Attachment A and will be referenced throughout the text. This attachment also contains more detailed instructions about the information to be included on the worksheets. Attachment C contains an example of the documentation produced during certification of a fictitious sensitive application.

The size and complexity of the security evaluation leading to certification will depend upon the numbers and types of functional security requirements defined by the users, auditors, or inspectors general. If few, relatively simple requirements are specified, it may be possible that the total project may be quickly completed by one person. In this case, it may not be necessary to complete all of the tasks listed in the detail specified. However, a decision to omit one or more of the tasks should be made only after carefully considering whether or not it is pertinent to the requirement. Obviously, a larger, more complex application with many security needs will require more time and other resources.

The methodology describes an approach geared to a new or substantially modified application. It is equally applicable to existing applications. In the latter case, one objective is to establish the documentation base-line which can be evaluated by the certifying official and, if acceptable, used as the basis for certifying the application. The existing security requirements should be reviewed to see if they have changed; existing safeguards must be documented and assessed for adequacy and finally, the safeguards must be tested to assure that they are performing as intended and to the satisfaction of the certifying official. These documents will then serve as the starting point for a subsequent re-certification.

Re-certification requires the execution of each step of the methodology to validate the earlier requirements, safeguards and findings, or to determine if requirements have changed. A major difference between certification and recertification is the existence of the documentation base-line which was developed during the initial certification or subsequent re-certification projects. These existing documents must be carefully evaluated at each step of the process. Changes, additions or deletions to the documents should be made to ensure that they truly reflect the present state of the application and its security-related capabilities or surroundings. It is possible that some steps may be omitted or abbreviated, but this should be done only after careful consideration of the intent of each step and ensuring that the supporting rationale will satisfy the certifying official.

**SENSITIVE APPLICATION CERTIFICATION
(NEW OR MODIFIED REQUIREMENT)**

(OMB Circular A-130)

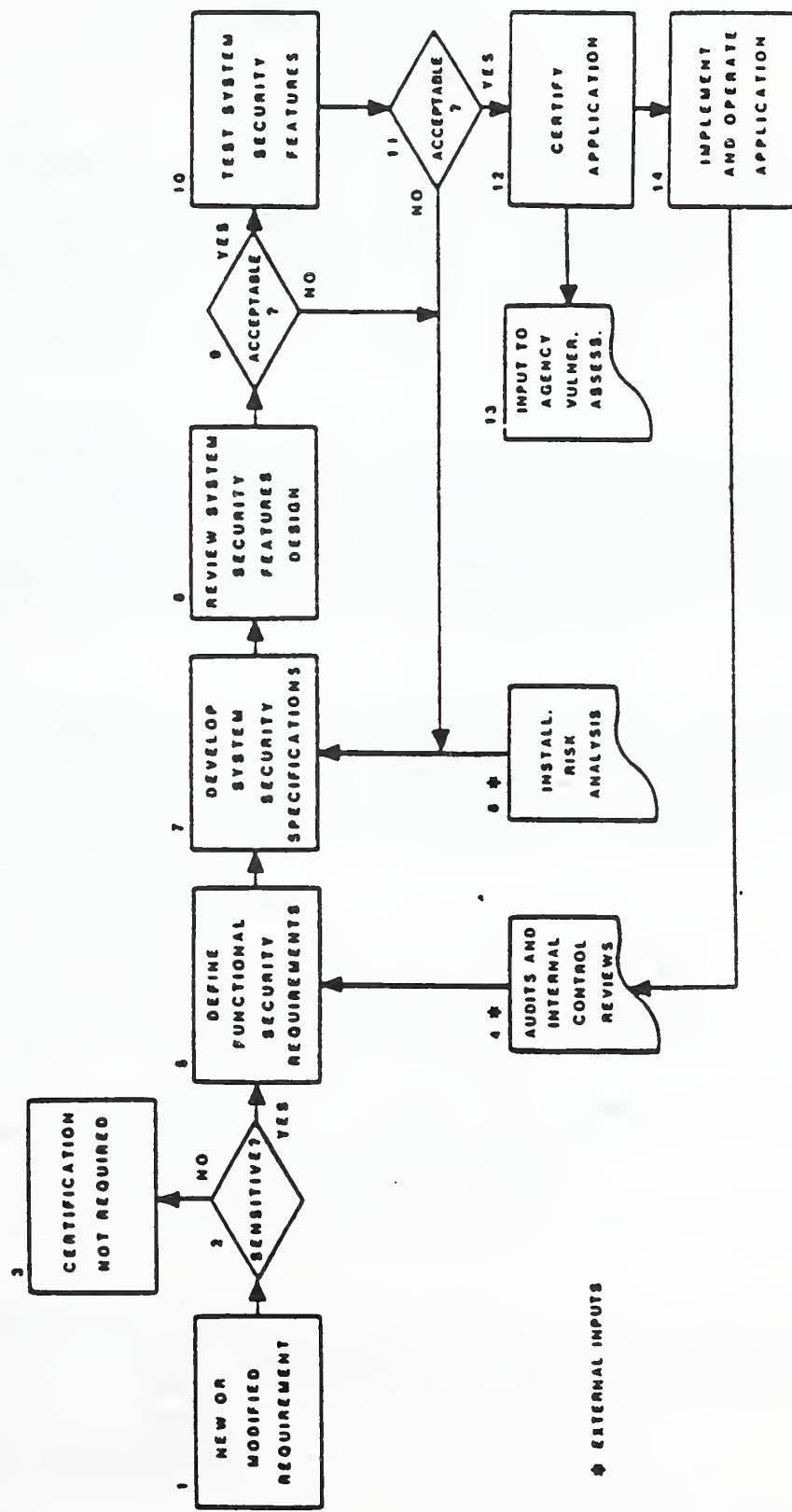
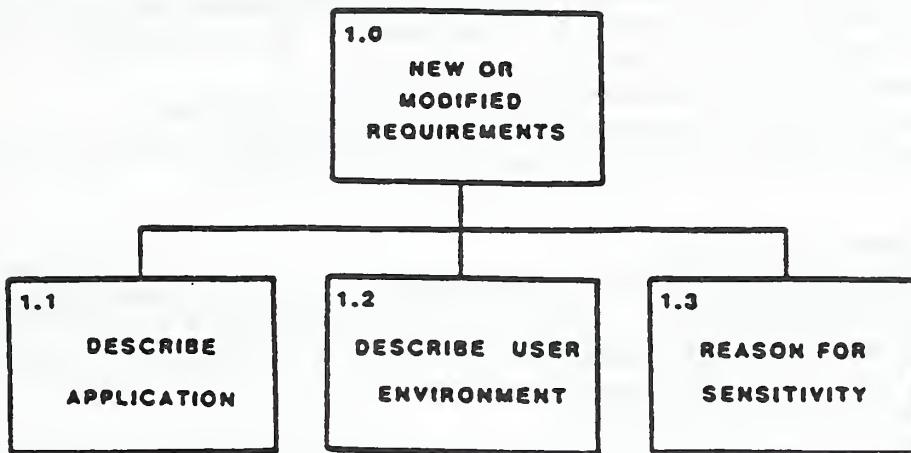


Figure V-1



1.0 New or Modified Requirement

Office of Management and Budget Circular A-130 directs that "agencies shall make the official whose program an information system supports responsible and accountable for the products of that system". Appendix III to the circular further states that "management officials who are the primary users of applications should evaluate the sensitivity of new or existing applications being substantially modified". By extension of these policies, the user officials, with their knowledge of the statutory, regulatory, and policy environment surrounding their application, are responsible for the identification of those applications requiring certification.

1.1 Describe Application

New applications, or existing applications which must undergo substantial changes, will be evaluated by the users to determine if they are sensitive or if their sensitivity has changed. Even though almost all applications are sensitive to some degree, most are not sufficiently sensitive to justify the lengthy and costly certification process. The selection of an application to be certified is a management decision that must carry with it a commitment of resources needed for the evaluation leading to certification.

- Inputs: Users knowledge and experience.
Outputs: Worksheet 1, Application Description.
Responsibility: Major using organization.
- User selects application which may require certification. (Note that within a system some applications may be sensitive while others are not).
- User enters the application title, application identification code recognizable to the computer (SYSID), and the names and telephone numbers of a knowledgeable functional and technical contact on Worksheet 1.
- On Worksheet 1 user describes in functional terms the nature of the application, how it supports the user, and its importance to the user.
- For existing applications, enter information as if this is a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current.

1.2 Describe the User Operating Environment

Briefly describe the user operating environment to include general user locations, type of support provided (e.g. batch or on-line), general access privileges or restrictions allowed or imposed, and any other information which may be of value in assessing the sensitivity of the application and its functional security needs.

- Inputs: Users knowledge and experience.
Outputs: Worksheet 1, Application Description.
Responsibility: Major using organization.

- Briefly describe the operational environment of the application within the user area(s). Give particular attention to area security, potential risks, and situations which may influence the need for adequate security. Enter this information in the space entitled "User Environment" on Worksheet 1. If necessary, continue on Worksheet 6.
- For existing applications, enter information as if this is a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current.

1.3 Indicate Reason for Sensitivity

The user will indicate the reason(s) why the application is considered sensitive, and an authoritative source if any, for this determination.

- Inputs: Users knowledge and experience.
Outputs: Worksheet 1, Application Description.
Responsibility: Major using organization.
- User records the reason(s) for the application sensitivity by checking the appropriate entry on Worksheet 1.
- If sensitive because of statute, regulation, or policy, list the source document.
- If deemed critical to a major DOC mission, indicate to whom critical.
- If sensitive for other reasons, explain.
- For existing applications, enter information as if this is a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current.

2.0
SENSITIVITY
DETERMINATION

2.0 Sensitive Determination

Based upon the information described above and documented on Worksheet 1 (Application Description), the user management may or may not decide that the application is sufficiently sensitive to warrant the expense of certification or re-certification. If it is decided that the application does not require certification, a record will be made of the decision and the certification of this application need not be continued.

- **Inputs:** Worksheet 1, Application Description.
- **Outputs:** Worksheet 1, Application Description.
- **Responsibility:** Senior user manager.
- A senior user manager will review the information collected and assess the sensitivity of the application.
- If the application is considered to be sufficiently sensitive to justify certification, the senior user manager will validate this by initialling the appropriate reason for sensitivity on Worksheet 1. This initiates the certification project and authorizes the full cooperation and support of the using organization.
- An Application Certification Manager will be designated to manage and coordinate the certification project. This individual may be selected from the using or the technical support (ADP) organization, at the option of the DOC agency.
- The Application Certification Manager will be given a written charter assigning responsibility and the authority to manage the project to a successful conclusion.
- The senior user manager will direct full cooperation of the using element for the remainder of the certification project.

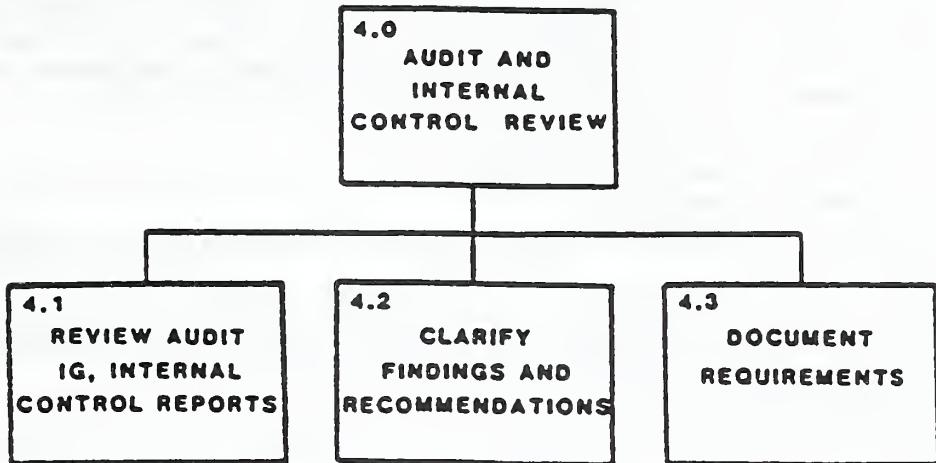
3.0

**CERTIFICATION
NOT REQUIRED**

3.0 Certification Not Required

If the application is determined to be non-sensitive within the context of OMB Circular A-130, or insufficiently sensitive to warrant the expense of certification, it will not be required. In this case, the decision and rationale must be documented and filed, available for subsequent audit or internal control review.

- Input: Worksheet 1, Application Description.
Outputs: Worksheet 1, Application Description.
Responsibility: Application Certification Manager.
- If determined to be non-sensitive, state this on Worksheet 1 or a continuation sheet (Worksheet 6) with the reasons for this determination.
- File the completed Worksheet 1 with the appropriate application documentation.
- Terminate the certification process for this application.



4.0 Audits, Inspections and Internal Control Reviews

Information which has been developed independently of this security evaluation must be considered by users in determining the security environment which must surround the application. These additional requirements may be found in audit, inspection and internal control reports. If security-related findings or recommendations are found and accepted, the appropriate technical, administrative, or physical safeguards must be included with the user requirements to be developed in Task 5.

4.1 Review Audit and Internal Control Reports

Review the reports of findings or recommendations which have an impact upon the accuracy, reliability, or security of the application. Identify those which appear to be appropriate for inclusion with the user functional security requirements of the application.

- Inputs: Worksheet 1, Application Description; Audits, inspections and internal reviews.
- Outputs: Worksheet 1, Application Description.
- Responsibility: Users.
- Collect and review audit, internal control reviews and inspectors general reports which pertain to this application.
- Identify and retain those findings or recommendations which have security implications for this application.
- For existing applications, enter information as if this is a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current.

4.2 Clarify Findings or Recommendations

If possible, discuss the pertinent findings and recommendations with the appropriate auditors or inspectors to ensure a complete understanding of their intentions. The auditor or inspector should be prepared to provide written descriptions of any recommended control or safeguard, its function, and the evidential proof needed to verify, to their satisfaction, its existence and effectiveness.

- Inputs: Worksheet 1, Application Description; Audits, inspections and internal reviews.
- Outputs: Worksheet 2, Security Requirements.
- Responsibility: Major user, auditors, and inspectors.

4.3 Document Audit or IG Requirements

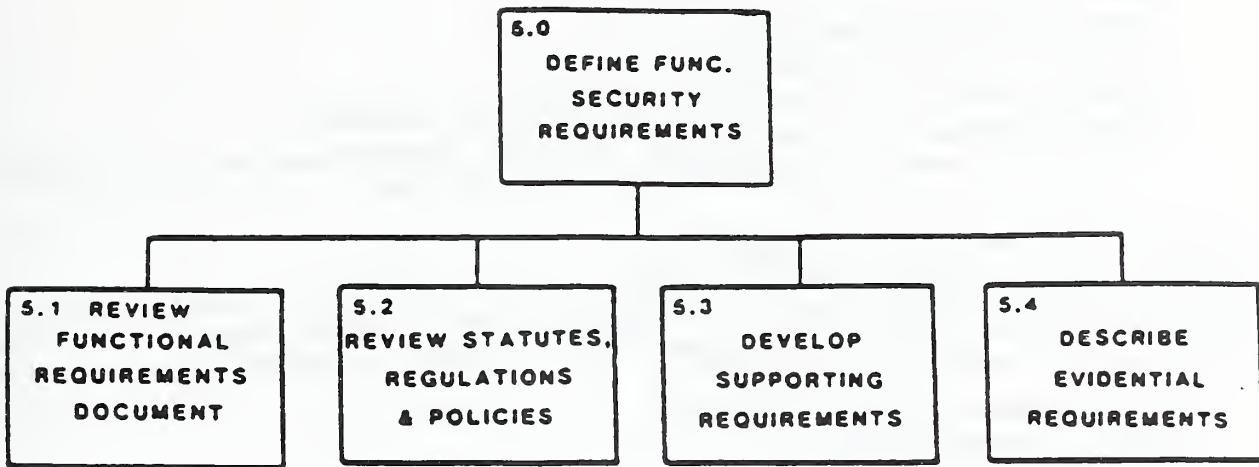
Recommendations which are security-related, appropriate for the application, and acceptable to the user will be completely described in functional, but specific, terms. The description must clearly state what

must be done to satisfy the recommendation. After describing the requirements for the security related feature which should be incorporated into the application or its operational environment, the auditor or inspector should then specify the "Required Evidence of Adequacy". This is a detailed description of the reaction or response of the "system" to prove the existence and effectiveness of the described feature or safeguard to the satisfaction of the auditor or inspector. If re-certifying an application, only the new or revised requirements need to be documented, but the earlier ones should be re-validated.

- Inputs: Worksheet 1 and approved requirements.
Outputs: Worksheet 2, Security Requirements.
Responsibility: Auditors, inspectors.
- Enter the application title, and the application identification code used by the computer (SYSID) on Worksheet 2.
- Each security-related requirement will be described on a separate copy of Worksheet 2. Each requirement will be assigned a unique number which will be entered on Worksheet 2 in the block titled "Func. Rqmt. #".
- Each security-related requirement must be accompanied by a detailed description of the evidence required to prove the existence and effectiveness of a proposed security feature which satisfies the requirement.

This information will be entered on the Worksheet 2 which describes that security requirement.

- For existing applications, enter information as if this is a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current.



5.0 Define Functional Security Requirements

Based upon knowledge of their sensitive data and the directives regarding its collection and use, users will define the security-related requirements and restrictions which must be incorporated into the application or its operational environment. These requirements will include those developed in Task 4 from audit or inspection reports. Each security-related requirement will be described in explicit detail, numbered uniquely, and may address any aspect of administrative, physical, or technical security, including accuracy and reliability of data or service. If the application is being re-certified, the existing requirements will be re-validated and new or revised requirements will be added or changed.

5.1 Review Functional Requirements Document

If a Functional Requirements Document (FRD) has been prepared it may contain detailed information about the security requirements of the application. These should be revalidated to ensure that they are complete and still appropriate, and incorporated into the requirements for this certification.

- Inputs: Worksheets 1 and FRD.
- Outputs: Worksheets 1 and 2.
- Responsibility: Major using organization.
- Enter the application title, and the identification code (used by the computer) in the block titled "SYSID" of Worksheet 2.
- Each security-related requirement will be described in functional terms on a separate copy of Worksheet 2 and will be numbered to provide a unique identification. This unique number will be entered within the block titled "Func. Rqmt. #", taking care not to duplicate requirement numbers already assigned.
- Each security-related requirement must be accompanied by a detailed description of the evidence required to prove its existence and effectiveness. This information will be entered on Worksheet 2.
- For existing applications, enter information as if this is a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current.

5.2 Review Pertinent Statutes, Regulations and Policies

If adequate security measures have not been specified in a Functional Requirements Document, or equivalent, the user should review the directives or policies which are pertinent to the application to identify any restrictions or security related requirements. If the intent of these is not clearly understood, assistance should be obtained from the legal, policy, inspector general or audit staff to ensure that the resulting application will also satisfy their requirements.

- Inputs: Worksheet 1 and pertinent directives.
Outputs: List of security-related requirements.
Responsibility: Major using organization.
- For existing applications, enter information as if this is a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current.

5.3 Develop Supporting Security Requirements

For each of the prohibitions, restrictions, or specific security requirements identified above, list in functional terms how the total "system" should handle each security relevant situation. The user should describe these requirements in their own functional but specific terms, each described on a separate copy of Worksheet 2 (Functional Security Requirement).

- Inputs: Worksheet 1 and list of requirements.
Outputs: Worksheets 1 and 2.
Responsibility: Major using organization.
- Enter the application title and the application identification code used by the computer (SYSID) in the appropriate blocks on Worksheet 2.
- Each security-related requirement will be entered and described on a separate copy of Worksheet 2 and will be uniquely numbered for identification. This unique number will be entered within the block titled "Func. Rqmt. #", taking care to avoid using requirement numbers already assigned.
- For existing applications, enter information as if this is a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current.

5.4 Describe Evidential Requirements

Each security control or safeguard is intended to elicit an expected system reaction or response to a given situation. These situations and responses must be described in detail for each requirement so that they can be used to prove the effectiveness of the controls. This "Required Evidence of Adequacy" should be described in the appropriate space on Worksheet 2, Functional Security Requirement.

- Inputs: Worksheets 1 and 2.
Outputs: Worksheets 1 and 2.
Responsibility: Major using organization.
- Each security-related requirement must be accompanied by a detailed description of the evidence needed to prove the existence and effectiveness of the required control or safeguard. This information will be entered on Worksheet 2.
- For existing applications, enter information as if this is a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current.



6.0 Review Installation Risk Analysis

Rather than install duplicative safeguards into each sensitive application, it is usually more cost-effective and efficient to incorporate a single safeguard which protects the larger operating environment of two or more applications. The installation risk analysis is intended to identify the need for this type of facility safeguard. (An example of the latter would be an uninterruptible power supply which can assure continuity of operations for all applications despite a power outage). The requirements identified by the users in Tasks 4 and 5 should be reviewed along with the risk analysis report to determine if some or all of the user needs have been satisfied by facility safeguards either existing or implemented as the result of the risk analysis.

6.1 Screen Functional Security Requirements

The user functional security requirements may have potential impact upon many areas: the using organization, the information technology facility, the guard force, couriers, or even external agencies. Since the risk analysis is primarily concerned with the security of the environment surrounding and within the information technology facility but not the applications, only those user requirements which could feasibly be satisfied by facility controls or safeguards need be considered in this sub-task.

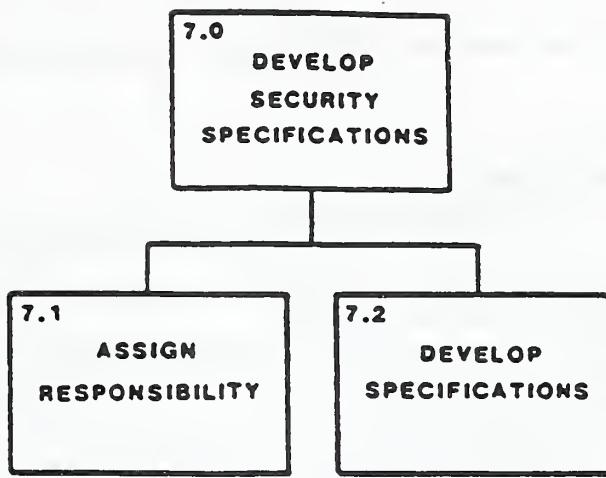
- Inputs: Worksheets 1 and 2; Installation Risk Analysis.
- Outputs: Worksheets 1 and 2.
- Responsibility: Information Technology staff.
- Screen each of the defined functional security requirements listed on Worksheets 2, selecting those which may be more appropriately satisfied by facility or system-wide controls or safeguards.

6.2 Identify Installation Controls or Safeguards

The technical staff will review each of the selected requirements to determine if existing facility controls or safeguards are present and adequate to satisfy the requirement. (If this appears to be true, it is advisable to obtain concurrence of the using organization to preclude later misunderstandings).

- Inputs: Worksheets 1 and 2; Facility Risk Analysis.
- Outputs: Worksheets 1 and 2.
- Responsibility: Information Technology staff.
- Review the findings of the facility risk analysis to identify those existing or subsequently implemented controls or safeguards which satisfy individual user requirements. Where adequate controls exist, its description should be entered on Worksheet 3 for subsequent evaluation during the design review (Task 8).

- Remaining unsatisfied requirements which may be common to two or more sensitive applications should be considered for facility-wide resolution, if feasible, otherwise the requirement must be included with the application requirements to be addressed in Task 7.0.
- For existing applications, enter information as if this is a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current.



7.0 Develop System Security Specifications

"Security specifications" are defined in OMB Circular A-130 as meaning a detailed, usually technical, description of the safeguards required to protect a sensitive application. An appropriate safeguard may be implemented within hardware or software, policies or procedures, communications, and a number of other possibilities. Because of this, each functional security requirement must be evaluated to determine how it can best be satisfied and by whom. Some will require the expertise of the information technology staff, while others may be more appropriately assigned to using or other organizational elements. After these assignments have been made, the responsible organizational staff must describe in explicit terms how the requirement can best be satisfied.

7.1 Assign Responsibility to Develop Security Specifications

Each unsatisfied functional security requirement will be reviewed to determine the skills and organization best suited to resolve the problem. For example, the need to relocate a guard may be assigned to the guard force supervisor; a policy or procedural change in the user area would be assigned to the user element; and the probable need for an access control software package would be assigned to the information technology staff. Occasionally, it may become necessary to negotiate the responsibility between organizations, but specific assignments must be made for each requirement.

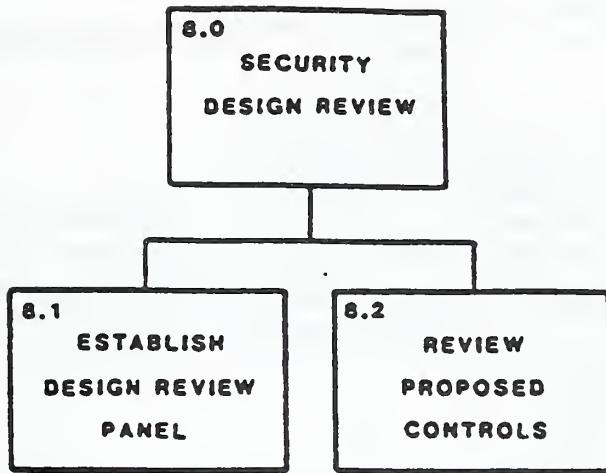
- Inputs: Worksheets 2.
- Outputs: Worksheet 2, responsibilities and deadlines.
- Responsibility: Application Certification Manager.
- Review each functional security requirement to determine the skills needed and functional area best suited to address the requirement.
- For existing applications, enter information as if this is a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current.
- Assign responsibility to devise an appropriate security feature and to develop specifications which will satisfy each functional security requirement. Each will be assigned to a specific individual or head of an organizational element.
- Establish deadlines for each requirement.

7.2 Develop Security Specifications

The organizations or individuals who have been assigned responsibility to develop the specifications for each new or revised security feature must devise an approach which will cost-effectively satisfy the requirement and provide the evidence necessary to prove or disprove its existence and effectiveness.

The solution for each requirement listed on the Worksheets 2 must be described in detail (with estimated costs, if possible).

- Inputs: Worksheet 2.
- Outputs: Worksheet 2 and 3.
- Responsibility: Designated individuals.
- Enter the application title, SYSID, and the functional requirement number in the appropriate spaces on Worksheet 3.
- Determine an appropriate and cost-effective control or safeguard to provide the degree of security warranted by the functional security requirement.
- Describe the proposed control or safeguard on Worksheet 3 in sufficient detail that its intents, purposes and capabilities will be clear to the design review panel and the individual(s) to be assigned to prepare or develop the feature.
- For applications to be re-certified, the existing controls must be reviewed and re-validated to ensure that they still satisfy the requirements for which intended. If appropriate, proposed revisions (or new controls) will be developed and described.
- If appropriate, prepare detailed specifications for the development or preparation of the proposed control or safeguard.
- The proposed solution must be reviewed by the appropriate supervisor or manager of the developing organization to assess its potential effectiveness, acceptability, and satisfaction of the requirement(s).
- Collect and assemble each functional security requirement (Worksheet 2), with the description of the proposed control or safeguard (Worksheet 3), for presentation to and consideration by the Design Review Panel.
- For existing applications undergoing an initial certification, treat as if a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, and current. If needed, revisions will be made to the earlier documents.



8.0 Proposed Security Features Design Review

After fully describing and/or preparing specifications for each proposed control or safeguard, they must be formally reviewed to assess their adequacy and acceptability both individually and collectively. (For applications being re-certified, only new or revised controls or safeguards need be evaluated in detail, but all should be considered to determine the overall security posture). The Design Review Panel will evaluate each of the features proposed (Worksheet 3) to satisfy the user requirements described on the accompanying Worksheet 2. The proposed contribution of these features to the overall security should be evaluated individually and collectively. The panel may approve unconditionally, approve on the condition that certain additional steps be taken, return for additional work, or determine that a given feature may not be needed because of the presence of other safeguards. The determination of acceptability must result from a decision that the proposed security controls or safeguards, individually and/or collectively, will provide the degree of security adequate for the sensitivity of the application.

8.1 Establish the Design Review Panel

Ideally, the Design Review Panel should be chaired by the certifying official since the acceptability or non-acceptability of the proposed security controls and safeguards, or any remaining risks, could be determined prior to incurring acquisition, preparation or development costs. Recognizing that this is not always possible, it is suggested that the panel be chaired by a senior manager of the using organization. This will be in keeping with the OMB policy holding the official whose program an information system supports responsible and accountable for the products (and acceptable security) of the application.

Other members of the panel will vary, depending upon the nature of the requirements and proposed solutions. If statutory matters are involved a member of the legal staff may be included. The audit and IG staff may also be represented, particularly if they have provided input or recommendations. Usually, the information technology staff will be involved as may be communicators, industrial security specialists, systems security specialists, and others. In other words, the composition of the panel must be determined on an application by application basis depending upon the nature of the requirements and proposed solutions to be evaluated.

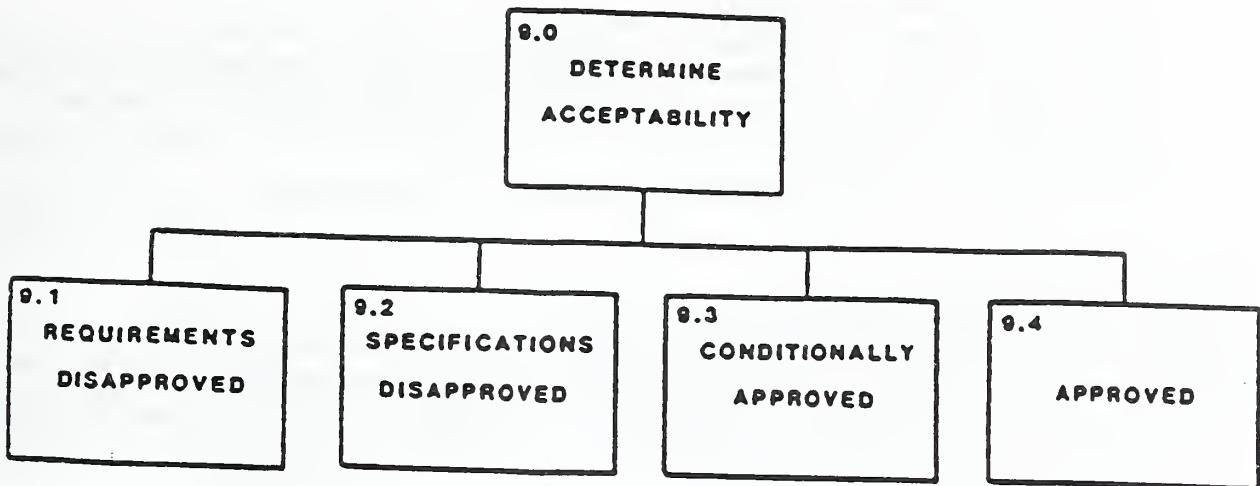
- Inputs: Worksheets 1, 2, and 3.
Outputs: Security feature Design Review Panel.
Responsibility: Certification Manager.
- Designate the person to chair the Design Review Panel.
- Review the security requirements and proposed controls or safeguard to determine the appropriate skills needed for the evaluation.
- Select appropriately skilled panel members.
- Schedule the review.

- Assemble the documents to be reviewed. (each requirement described on Worksheet 2 followed by its proposed solution on Worksheet 3).

8.2 Review Proposed Security Controls or Safeguards

The panel will review and validate, if appropriate, each functional security requirement. Then, the proposed security control or safeguard will be evaluated to ascertain its likelihood of satisfying the requirement. Finally, the panel will review the "Required Evidence of Adequacy" to determine if it appears that the proposed security feature can satisfactorily provide the proof needed to validate its existence and effectiveness. (For applications being re-certified, the new or revised requirements, controls or safeguards will be examined in detail in conjunction with the existing ones).

- Inputs: Worksheets 2 and 3.
- Outputs: Worksheets 2 and 3.
- Responsibility: Design Review Panel.
- The panel will review each functional security requirement, obtaining additional information from the user representative, if needed.
- The panel will review each proposed control or safeguard to determine whether it will satisfy the requirement. The designer of the control or safeguard will provide additional information, if needed.
- The panel will review the proposed "Required Evidence of Adequacy" to assess its validity to prove that the control or safeguard is present and operating effectively, and the likelihood that it will produce this evidence.
- For existing applications undergoing an initial certification, treat as if a new application.
- When re-certifying an application, review information collected during the last certification or re-certification to ensure that it is still complete, correct, current and acceptable.



9.0 Determine Acceptability

The Design Review Panel will assess each proposed control or safeguard, as well as existing ones, to determine its acceptability to provide a level of protection equal to or greater than that specified by the users. The panel may approve, disapprove, or approve conditionally, with appropriate reasons stated for the latter two decisions. The decision and appropriate comments will be entered on Worksheet 3, and disposition of the document(s) will be as determined by the decision and reasons given.

9.1 Disapproved Requirements

Functional security requirements which are considered inadequate, or which represent an unacceptable level of risk, will be returned to the functional contact listed on Worksheet 1 for further analysis and/or rebuttal of the decision. The rebuttal may be added as a continuation sheet to the appropriate Worksheet 2, or may be in the form of completely new requirements, required evidence of adequacy, or description of security feature. The new information will be documented and returned to the panel for reconsideration.

- Inputs: Disapproved requirements on Worksheets 2 and 3.
Outputs: New or revised Worksheets 2 and 3.
Responsibility: Proponent of requirement.
- If the Design Review Panel determines that the functional security requirement (Worksheet 2) is erroneous, inadequate, or represents an unacceptable level of risk, the requirement will be returned to the originator of the requirement with the reasons for the decision.
- The originator of the requirement may defend the requirement by a rebuttal to the panel, either in writing or in person.
- The originator may revise the requirement to make it acceptable and return to the panel for reconsideration.
- The originator of the requirement may opt to accept the risk presented by the omission of the control or safeguard.

9.2 Disapproved Specifications

If the panel determines that the specifications for the proposed, revised or existing solution to the security requirement are inappropriate or inadequate, Worksheets 2 and 3 will be returned to the developer of the specifications, with the reasons for disapproval. If revision of the specifications are indicated, they will be revised and resubmitted to the panel for reconsideration.

- Inputs: Disapproved Worksheets 2 and 3.
Outputs: New or revised Worksheets 2 and 3.
Responsibility: Developer of specifications.

- If the Design Review Panel determines that the security feature specifications (Worksheet 3) are erroneous, inadequate, or represent an unacceptable level of risk, the appropriate Worksheets 2 and 3 will be returned to the originator of the specifications with the reasons for the decision.
- The originator of the specifications may defend the proposed feature by a rebuttal to the panel, either in writing or in person, or
- The originator may revise the specifications to make them acceptable and return to the panel for reconsideration.

9.3 Conditionally Approved

In these cases, the requirements and proposed specifications for the new, revised, or existing solution are approved on condition that certain controls or restrictions be placed on operation of the application. The functional security requirement, evidential requirement, and proposed control or safeguard specifications will be returned, along with the directed conditions, to the organization or individual who can satisfy the conditions. Subsequently, the revised document will be resubmitted for reconsideration.

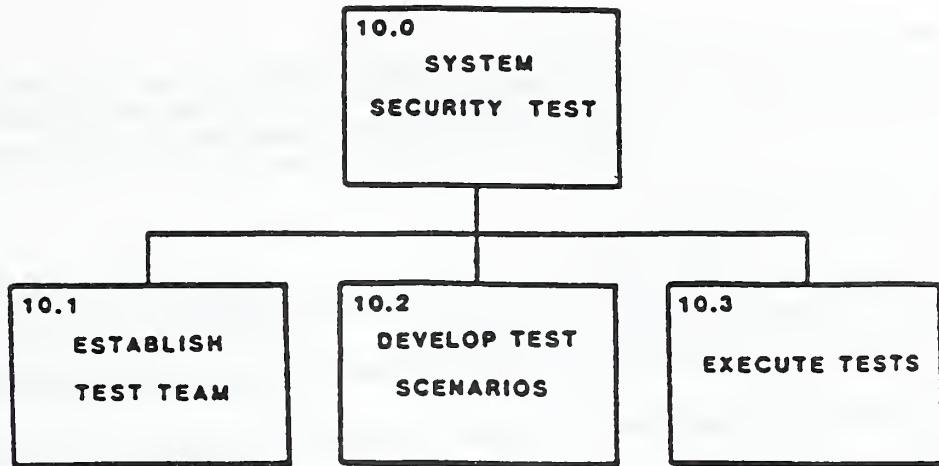
- Inputs: Worksheets 2 and 3 with conditions.
Outputs: New or revised Worksheets 2 and 3.
Responsibility: Appropriate individual.
- If the Design Review Panel determines that the requirement and proposed security feature is unacceptable within certain stated conditions, the Worksheets 2 and 3 will be returned to the individual who has the authority and/or skills to satisfy those conditions.
- This individual may defend the proposal by a rebuttal to the panel, either in writing or in person, or
- The originator may revise the documents to make them acceptable and return to the panel for reconsideration, or
- The originator may satisfy the conditions, stating this on Worksheet 3, and return to the Design Review Panel.

9.4 Approved Requirements and Security Features

The controls or safeguards which were initially or subsequently approved must be developed or prepared and implemented. The organizational element that will be responsible for each of these will depend upon the nature of the approved feature, these actions may range from developing an administrative procedure, preparing a computer program, installing physical devices, or any number of other actions. The responsibility for developing or preparing and implementing each security control or safeguard must be specifically assigned and monitored until all have been implemented. (Care must be taken not to overlook those which have been returned to the originators for revisions).

(NOTE: At this point, the certification process may be interrupted to permit preparation or development and implementation of the new or revised controls or safeguards approved by the Design Review Panel).

- Inputs: Worksheets 2 and 3.
Outputs: Implemented controls or safeguards.
Responsibility: Designated individuals.
- The Application Certification Manager will designate the organizations or individuals to develop or prepare and implement each of the approved new or revised security features.
- These organizations or individuals will develop or prepare, unit test if appropriate, and implement the new or revised security features for which responsible, notifying the Application Certification Manager as each is implemented.



10.0 System Security Test

OMB Circular A-130 specifies that all agencies shall conduct systems tests prior to placing a sensitive application into operation, to assure that the proposed design meets approved security specifications. By implication, an existing application or one to be re-certified also must undergo a systems test to prove that the existing, new, or revised controls or safeguards are operating as intended. The objective of these tests is to verify that required administrative, technical, and physical safeguards are installed and are operationally effective. The tests and results shall be fully documented and maintained in the official application records as a part of the certification or re-certification documentation, subject to audit or internal control review.

10.1 Establish a Test Team

The test team will design, develop and/or execute test scenarios intended to ensure that the new, revised, or existing security controls and safeguards are in place and can demonstrate their effectiveness by satisfying the evidential requirements. Because of the wide range of skills which could be needed, the specific complement of each team must be individually determined for each application, depending upon the nature of the tests to be developed and executed. In consonance with the policy to hold user management responsible for the security of their applications, it is suggested that the test team leader be a senior manager. The members of the team may require skills in the areas of software, communications, industrial security, user function(s), or other specialties. The test team members must be qualified to devise and execute tests to prove or disprove satisfaction of the functional security requirements.

- Inputs: Worksheets 2 and 3.
Outputs: Test Team complement.
Responsibility: Certification Manager.
- Designate the test team leader.
- Divide the requirements and proposed security controls and safeguards into categories representing the disciplines needed to develop or evaluate test scenarios (e.g. operating and utility systems, applications development, data communications, industrial security, user procedures, etc.)
- Designate the individuals who possess the appropriate skills to develop (and execute), or evaluate, test scenarios for each of the categories.
- Assign responsibilities for evaluation or development and execution of the test scenarios.

10.2 Develop Test Scenarios

The test team members will develop appropriate tests to fully exercise the new or revised security features, and to evaluate and execute existing tests which were developed earlier and re-validated. Each

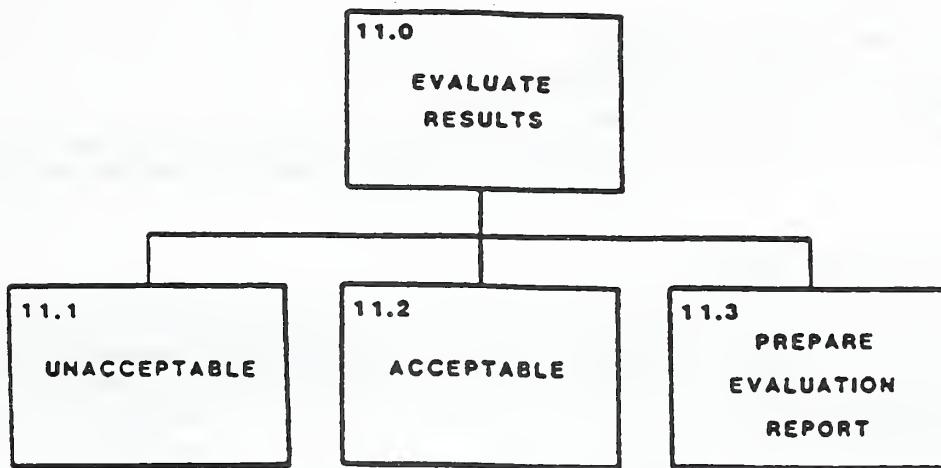
test must ensure that each security control or safeguard: satisfies the user requirements for which it is designed; is in accord with the approved specifications; and provides the proof of adequacy specified by the user. A test may exercise one or more of the security features, either partially or totally. If partially, additional tests must ensure a full evaluation of the adequacy of the feature.

- Inputs: Worksheets 2 and 3.
Outputs: Worksheets 2, 3, and 4.
Responsibility: Test Team members.
- Study the security control or safeguard description, specifications, and the proof of adequacy which must be demonstrated for each situation.
- Determine the type of test needed to prove the presence and effectiveness of each control or safeguard.
- Group together those related security controls or safeguards which may be evaluated by a common test.'
- For applications being re-certified, the existing tests must be re-validated to ensure that they are still appropriate and effective.
- Enter the application title, SYSID and functional requirement number on Worksheet 4.
- A Worksheet 4 will normally be required for each security feature to be tested.
- A Worksheet 4 will be required for each test scenario.
- If more than one test is needed to satisfy a single requirement, number each test scenario for identification and enter this number in "Test" on Worksheet 4. Each of these tests should be documented on a separate worksheet.
- Develop a step-by-step detailed description of the test and document this in the "Test Scenario" column on Worksheet 4.
- Where specific responses or reactions are to be expected from the "system", describe the situation which is intended to produce the response, when (in the process) the response is expected, and the specific response expected.

10.3 Execute Tests

After all test scenarios have been designed and documented, or re-validated, on Worksheet 4, and the necessary test preparations have been completed, each will be executed and the results entered on the worksheet opposite the test step where the results were obtained.

- Inputs: Worksheet 4.
Outputs: Detailed results of tests.
Responsibility: Test Team members.
- Group the test scenarios by the areas to be tested (e.g. physical plant, software, procedures, communications, etc).
- Assign one or more individuals to be responsible for executing the tests for each area.
- Execute each step of each test, recording the results achieved alongside the step which produced the results on Worksheet 4.
- If inadequate or undesired results are produced and subsequently determined to be caused by a faulty or improperly designed test, the test must be revised and executed until its reliability has been proven.
- If inadequate or undesired results are produced, and the test is considered to be reliable, the known or suspected cause of the results should be recorded on the worksheet for subsequent analysis.



11.0 Evaluate Results for Acceptability

The results of each test will be evaluated to ascertain that the security feature functioned as intended; produced the required evidence of adequacy; and satisfied the functional security requirements of the user. The evaluation of each test will be recorded on a separate Worksheet 5 for each test scenario.

11.1 Results are Unacceptable

Where unacceptable results were obtained, the test will be reviewed to determine its correctness and reliability, to be followed by revisions and a retest, if appropriate. If the results are still unacceptable, a revision of the feature specifications may be required, or the proof of adequacy may be in error. These will be corrected and followed by a retest; or, the user may opt to omit the control or safeguard and accept the risk involved.

- Inputs: Worksheets 2, 3, and 4.
- Outputs: Security features appearing unacceptable.
- Responsibility: Test team manager and members.
- Identify those tests which produced unacceptable, incomplete, or unpredicted results.
- Review the test to ensure that it is designed to fully test the security feature and that the appropriate parameters or indicators were tested and presented. If the test is faulty or inadequate it must be revised and the feature retested until reliable results are achieved.
- After the test reliability has been established, if the results are still unacceptable the specifications for the security feature and the way it was implemented must be evaluated to determine whether: 1) the specifications are complete and correct, or 2) the feature was correctly implemented. This should be a joint effort between the appropriate member of the test team, the developers of the security feature specifications, and the developer or implementor of the feature.
- If the absence of this security feature will pose a substantial and unacceptable risk, the specifications and/or implementation of the feature must be revised and retested until correct and acceptable results are achieved.
- If the absence of this security feature will pose a relatively minor risk, possibly due to the presence of other security features, the team may decide to recommend acceptance of the risk, or acceptance based upon the imposition of certain conditions or restrictions. User management must concur in this recommendation.
- Remaining risks, if any, must be identified and listed in order of potential harm for inclusion in the evaluation report. Recommendations or corrective actions should be developed for each remaining risk and recorded on the Worksheet 5 for that specific test.

11.2 Results are Acceptable

Tests which initially or subsequently produce acceptable results should be thoroughly reviewed to ensure that each operated correctly and provided the required evidence of adequacy of the security feature.

- Inputs: Worksheets 2, 3, 4, and 5.
Outputs: Features proven acceptable.
Responsibility: Test team manager and members.
- The results of this analysis will be entered on Worksheet 5 and appended to the appropriate functional security requirement (Worksheet 2) and its supporting documentation (Worksheets 3 and 4).

11.3 Prepare Evaluation Report

When all test results are within acceptable limits, or the user opts to recommend acceptance of any remaining risks, the test team will prepare an evaluation report. This document will consist of both summary and detailed information upon which the certification official can base a decision.

- Inputs: All worksheets.
Outputs: Evaluation Report.
Responsibility: Certification Manager, Test Team Manager, user management, and any other functional or technical specialists who may be required to assist.
- Prepare Evaluation Report Similar to Below:

1. **Introduction and Summary:** Briefly describe the application and its purpose in functional terms (See Worksheet 1); its importance to the organization; the reasons for its sensitivity; and summarize both the positive and negative aspects of the overall evaluation findings and recommendations.
2. **Background:** Describe in fairly general terms the potential impact(s) of a serious breach of security. Also describe in general terms the security environment surrounding the application, but not a part of the application (e.g. facility or communications security), which contribute to the security or vulnerability of the application. Define the boundaries of the certification project (what was and what was not included), and any other information which may assist the certifying official to understand the scope and importance of the project.
3. **Major Findings:** Summarize the major controls and safeguards which are in-place and their general role in protecting assets and preventing data disclosure, alteration, destruction, or manipulation. Also discuss the remaining vulnerabilities of the application and threats which may be brought to bear on them. Vulnerabilities should be discussed in terms of those which are considered reasonably acceptable, and those which require further protection.
4. **Recommended Corrective Actions:** This section should start with the overall certification recommendation(s) of the team. The team may recommend unqualified certification for operation; certify the application subject to certain restrictions or conditions; or recommend that the application not be certified for cause. Specific recommended corrective actions, if any, will be listed in order of their contribution to the overall security of the application. Each recommendation should include an estimate of the cost or other resources associated with its implementation, and the suggested organizational element which should be assigned responsibility.
5. **Certification Process:** The purpose of this section is to describe the certification process so that the certifying official can assess the confidence to be placed in the findings and recommendations.
6. **Attachments:** The following information shall be appended to the evaluation report.

Proposed Certificate. This certificate, prepared for the signature of the certifying official, will embody the overall recommendation of the evaluation team, and may include proposed restrictions or conditions as well as recommended corrective actions. Naturally, these are subject to approval or revisions by the certifying official. (See example at Attachment B).

Certification Documents. The documents developed during the project (completed worksheets), properly assembled, will be appended to the evaluation report. This is for the benefit of the certifying official or any other authorized person who requires more detailed information about any aspect of the definition, development, or testing of the security controls or safeguards.



12.0 Certify Application for Operation

The Certifying Official will review the evaluation report prepared by the team and may: fully approve for implementation and operation; approve with specified restrictions or conditions; or disapprove and return with the reasons for disapproval. In the latter two cases, the reasons stated will determine what, if any, additional action will be required.

- Inputs: Evaluation Report and Attachments.
Outputs: Certification or other decision.
Responsibility: Certifying Official.
- If approved for implementation and operation, the certifying official will sign the certificate and send a copy to the major user of the application. The original certificate and supporting documentation will be retained in the application documentation. A copy of the signed certificate and the evaluation report will be given to the organizational element(s) responsible for performing internal reviews in accord with OMB Circular A-123.
- If approved with conditions or restrictions, the same procedure will be followed, but the application must be operated within those conditions or restrictions. Compliance will be evaluated during periodic audits, inspections, or internal control reviews.
- If disapproved, the application will not be implemented until the reasons for disapproval have been eliminated or ameliorated to the satisfaction of the certifying official.

13.0
VULNERABILITY
ASSESSMENT

13.0 Vulnerability Assessment

Any conditions or restrictions stated on the certificate, and the supporting security evaluation documents, will be considered during the vulnerability assessment and internal control reviews conducted in accordance with OMB Circular A-123. Significant security or other control weaknesses which were identified and still remain shall be considered for inclusion in the annual internal control review assurance letter and report required by the circular.

- Inputs: Copy of Certification documentation.
Outputs: Agency Vulnerability Assessment.
Responsibility: Designated organization.
- The functional element responsible for the overall vulnerability assessment and internal control reviews will consider any significant weaknesses contained within the certification documentation for possible inclusion in the annual reports.

14.0
IMPLEMENT
AND OPERATE
APPLICATION

14.0 Implement or Continue to Operate Application

When certified or conditionally certified, the application may be implemented, or continued in a production mode subject to standard DOC policies and procedures, and any conditions or restrictions imposed by the certifying official.

VI. RECERTIFYING A SENSITIVE APPLICATION

A. Requirement for Re-Certification

OMB Circular A-130 states that agencies shall conduct periodic audits or reviews of sensitive applications and recertify the adequacy of security safeguards. It directs that these applications be recertified at least every three years. By implication, this presumes that an initial security evaluation was performed earlier and that the sensitive application was certified (or recertified) for full or conditional operation. For this reason, the security evaluation leading to recertification will start with a fairly substantial, if not complete, documentation base.

B. The Approach

1. The recertification process is essentially the same as that used for initial certification. (See Figure VI-1). The major difference is that many, if not all, of the security requirements, controls and safeguards may have already been defined, developed, implemented and certified. Since the last evaluation, however, many changes to the user and operating environments may have occurred. The purpose of recertification is to detect these changes and to evaluate their effect upon the security, accuracy and continued availability of the data and the supporting resources. Recertification requires:
 - a. A review of functional security requirements to see if any have changed or new requirements have arisen;
 - b. Reassessment of the vulnerabilities and threats to sensitive data and supporting resources which may have arisen or changed since the last evaluation;
 - c. Re-evaluation of the implemented controls and safeguards to assure that they are still functioning properly; and,
 - d. The identification and implementation of new or revised controls or safeguards which may be required as the result of the latest evaluation
2. The recertification process must be documented for retention, replacing the earlier certification or re-certification evaluation. The methodical approach described in this document should still be used to re-certify a sensitive application in order to ensure that the existing controls and safeguards are still current, complete, and operate correctly. The results of the re-certification findings will be documented as described in Section V for the initial certification, using, revising, and updating existing documents to the maximum extent practical. The test results, however, cannot be re-used since the re-validated tests must be re-executed to prove the continued presence and effectiveness of the installed controls and safeguards.
3. Although recertification may appear to be a formidable undertaking, it may be relatively easy if the previous certification (or recertification) was properly done and documented. Since a major portion, if not all of the documentation will be available from the earlier certification (or re-certification), re-certification should require considerably less time and other resources. The important thing is that each step is executed to the degree necessary to ensure that significant requirements which may have arisen or revised since the last certification/recertification have been identified and accommodated.
4. Review Figure VI-1 to note the relatively minor differences between the initial certification and recertification (for example, "Define Functional Security Requirements" vis-a-vis "Revise or Re-Validate Functional Security Requirements"). After noting and understanding the minor differences in the approaches, the recertification project can be started with the appointment of an Application (Re-)Certification Manager to be responsible for execution of the methodology as described in Section V.

SENSITIVE APPLICATION RECERTIFICATION

(OMB Circular A-130)

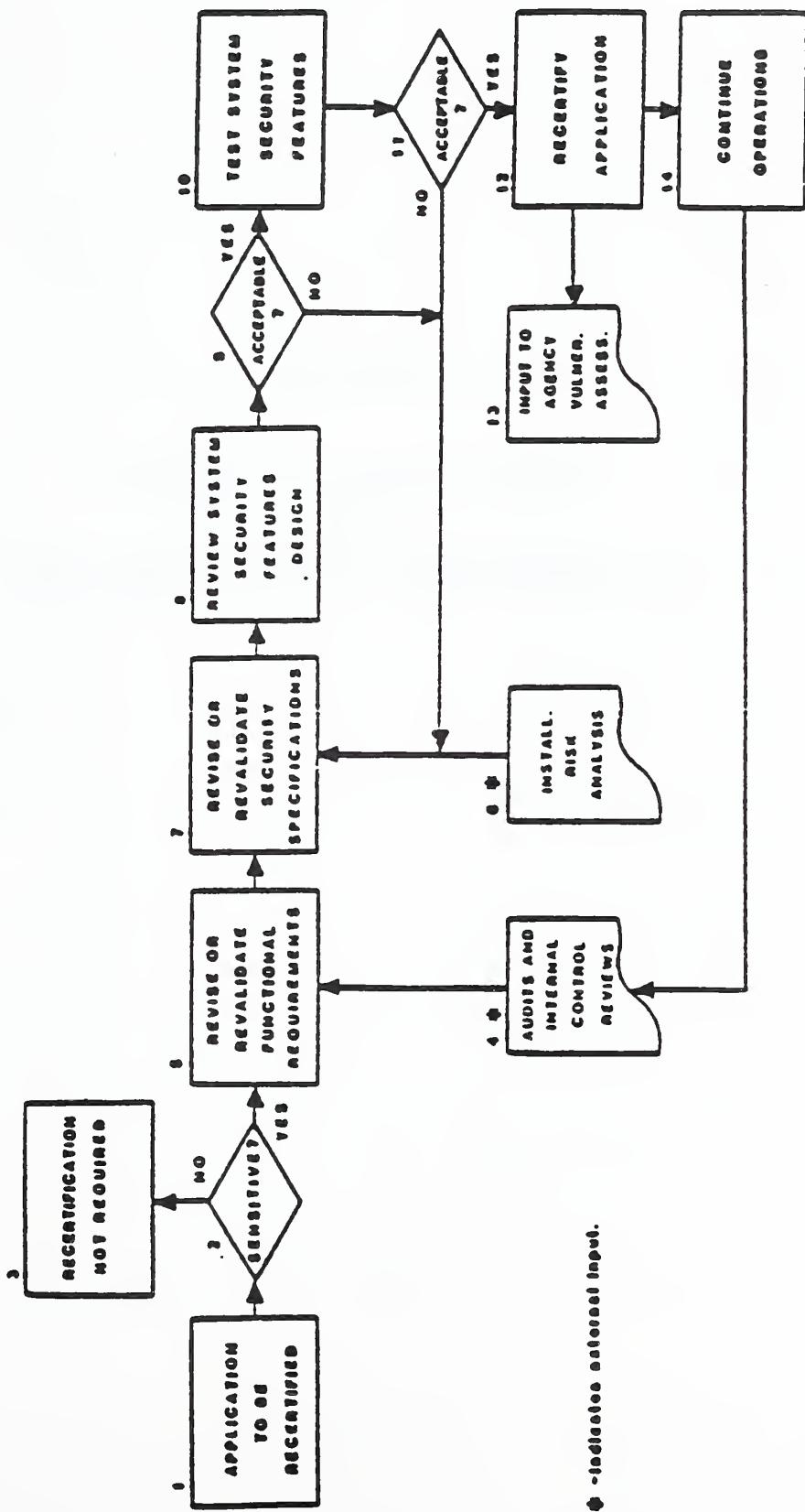


Figure VI-1

ATTACHMENT A

**SUGGESTED WORKSHEETS
FOR
SENSITIVE APPLICATION
CERTIFICATION OR RECERTIFICATION**

SUGGESTED WORKSHEET ENTRY DESCRIPTIONS

The following are explanations of the entries to be made on the suggested worksheets. The number of each explanation relates to the circled number on the attached forms.

- 1. Worksheet Number:** Pre-printed in the upper right hand corner of each worksheet.
- 2. System/Application Title:** The descriptive title used to identify the application to be certified or recertified.
- 3. SYSID:** The identification code used by the computer to uniquely identify this application from all others.
- 4. Func. Contact:** The name and telephone number of the person within the using organization to serve as the official point of contact, and coordinate all user actions required of that organization.
- 5. Tech. Contact:** The name and telephone number of the person within the information technology organization who is most knowledgeable about the application and will coordinate the actions required of that organization.
- 6. Brief Functional Description:** A description of the application in user terms, explaining the purpose of the application; its importance to the user; generally how the data is used; and, similar information to serve as the basis of understanding for all individuals to be involved in the certification or recertification project.
- 7. User Environment:** In user terms, generally describe the type of support provided (e.g. batch, on-line, frequency used, etc); general restrictions or privileges required; physical environment; and any other general information which will be of value in assessing the vulnerabilities of the application within the user areas.
- 8. Reason for Sensitivity:** Enter the reason why the application, its data and resources, should be considered as sensitive. If required by an official document, list the document. If critical to performing a major mission, indicate the organizational element most responsible for performing that mission.
- 9. Func. Rqmt. #:** A unique number assigned to each functional security requirement which must be accommodated by some portion of the total "system" surrounding or a part of the application.
- 10. Description of Functional Security Requirement:** A security related requirement expressed in user terms, describing specific authorizations, restrictions, privileges, accesses, edits, reasonableness tests, ranges, processes, results or similar requirements which are intended to ensure the security, quality, availability, and reliability of the data and supporting resources. Each functional security requirement should be listed and described separately.
- 11. Required Evidence of Adequacy:** The required response(s) or reaction(s) which must be evidenced by the overall application "system" in a given situation to prove that one or more of the security features are performing as intended to satisfy the functional security requirement. The situation(s) must be described in detail, followed by the response or reaction which should ensue.
- 12. Description of Security Feature:** The detailed description of a control or safeguard intended to provide the protection, detection or control needed to satisfy one or more of the functional security requirements. The description should be sufficiently detailed to permit an evaluation by the Design Review Panel, and to provide detailed instructions to the individual who will be assigned the responsibility to develop and/or implement the control or safeguard.
- 13. Design Review:** This block is intended to record the decision of the Design Review Panel. The chairperson will record the decision of the panel with regard to each proposed control or safeguard. If other than "approved", the decision must be accompanied by appropriate and definitive remarks to explain the reasons for the decision and what must be done to arrive at an acceptable proposal.
- 14. Test Scenario:** A documented, step-by-step series of actions designed to prove or disprove that the implemented controls or safeguards are present and performing as required and

specified. These will include situations which are intended to produce specific responses, and the responses expected.

15. **Test Results:** Specific responses or reactions which are produced for given situations (test scenarios) at a particular point in time, process, or space as defined in the test scenario.
16. **Test #:** If more than one test is required to exercise a specific security feature, each must be assigned a unique identifying number.
17. **Evaluation of Test Results:** Each test will be evaluated separately on Worksheet 5. This entry will contain an assessment of the security feature performance against the requirements (specifications), along with any strengths or weaknesses found. Recommendations pertaining to the evaluation of the results for that particular test will be entered here.
18. **Recommendations:** A recommendation should be entered on Worksheet 5 for each of the tests performed. This may be a recommendation for full acceptance, total rejection, or some point in between. In cases of conditional acceptance or recommended rejection, corrective actions should be proposed.
19. **Continuations:** This worksheet may be used to extend any block on any form. The appropriate referencing information should be entered at the top of the worksheet, followed by the title of the continued block, and the extended information.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

(APPLICATION DESCRIPTION)

1

1

SYSTEM/APPLICATION TITLE

2

SYSID

3

FUNC. CONTACT:

4

TECH. CONTACT

5

BRIEF FUNCTIONAL DESCRIPTION:

6

USER ENVIRONMENT

7

REASON FOR
SENSITIVITY:

STATUTE (LIST): _____

8

POLICY (SOURCE): _____

CRITICAL TO (AGENCY & DEPT.): _____

OTHER (EXPLAIN): _____

SENSITIVE APPLICATION CERTIFICATION WORKSHEET (FUNCTIONAL SECURITY REQUIREMENT)



SYSTEM/APPLICATION TITLE	SVSID	FUNC. RQMT. #
②	③	④

DESCRIPTION OF FUNCTIONAL SECURITY REQUIREMENT

⑩

REQUIRED EVIDENCE OF ADEQUACY

⑪

SENSITIVE APPLICATION CERTIFICATION WORKSHEET (SECURITY FEATURE SPECIFICATIONS)

3

1

SYSTEM/APPLICATION TITLE

2

SYSD

FUNC. RQMT. #

3

9

—

DESCRIPTION OF SECURITY FEATURE

12

DESIGN REVIEW

13

 APPROVED CONDITIONALLY APPROVED (Explain) DISAPPROVED (Explain)

SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(SECURITY TESTS)

4



SYSTEM/APPLICATION NAME	②	SYSID	FUNC. NAME	TEST ✓
		③	④	⑩

TEST SCENARIO	⑮
	⑯

TEST RESULTS	⑰
--------------	---

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

(EVALUATION)

5



1

SYSTEM/APPLICATION TITLE

2

STASIS	FUNC. BOMT. +	TEST +
3	9	16

EVALUATION OF TEST RESULTS

17

RECOMMENDATIONS

18

SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(CONTINUATION SHEET)

6



SYSTEM/APPLICATION TITLE	SYSIO	FUNC. ROMT.✓	TEST ✓
	3	9	16

19

2

1

SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(APPLICATION DESCRIPTION)

SYSTEM/APPLICATION TITLE		SYSID		
FUNC. CONTACT:		TECH. CONTACT		
BRIEF FUNCTIONAL DESCRIPTION:				
USER LOCATIONS:				
REASON FOR SENSITIVITY: ____ STATUTE (LIST): _____ ____ POLICY (SOURCE): _____ ____ CRITICAL TO (AGENCY & DEPT.): _____ ____ OTHER (EXPLAIN): _____				

2

**SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(FUNCTIONAL SECURITY REQUIREMENT)**

SYSTEM/APPLICATION TITLE	SYSPID	FUNC. RQMT. #	
			—

DESCRIPTION OF FUNCTIONAL SECURITY REQUIREMENT

REQUIRED EVIDENCE OF ADEQUACY

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

(SECURITY FEATURE SPECIFICATIONS)

3

SYSTEM/APPLICATION TITLE	SYSID	FUNC. RQMT. #	

DESCRIPTION OF SECURITY FEATURE

DESIGN REVIEW

APPROVED

CONDITIONALLY APPROVED (Explain)

DISAPPROVED (Explain)

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

(SECURITY TESTS)

4.

SYSTEM/APPLICATION TITLE	TEST SCENARIO	TEST RESULTS	ACTION	REASON	TESTER	TESTER SIGNATURE
		- VOID	FUNC. ROMT. ♦			

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

(EVALUATION)

5

SYSTEM/APPLICATION TITLE	SYBID	FUNC. ROUT. #	SCENARIO #

EVALUATION OF TEST RESULTS

RECOMMENDATIONS

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

6

(CONTINUATION SHEET)

SYSTEM/APPLICATION TITLE

SYSID

ATTACHMENT B

EXAMPLES OF CERTIFICATION STATEMENTS

EXAMPLE OF CERTIFICATION STATEMENT

I have carefully examined the certification findings and recommendations documented in the (application name) security evaluation report, dated _____. Based on my authority and judgment, and weighing the remaining residual risks against operational requirements, I authorize continued operation of (application name) under the following restrictions or conditions.
(List restrictions or "None")

I further authorize initiation of the following corrective actions.
(List corrective actions or "None")

(Signature and date)

EXAMPLE OF RECERTIFICATION STATEMENT

I have carefully examined the recertification findings and recommendations documented in the (application name) security evaluation report, dated _____. Based on my authority and judgment, and weighing the remaining residual risks against operational requirements, I authorize continued operation of (application name) under the following restrictions or conditions.
(List restrictions or "None")

I further authorize initiation of the following corrective actions.
(List corrective actions or "None")

(Signature and date)

ATTACHMENT C

**EXAMPLE OF COMPLETED
WORKSHEET SAMPLES**

EXAMPLE OF COMPLETED WORKSHEET SAMPLES

The following pages contain an example of a certification project to show how completed documents may appear. Naturally, the details of the entries will vary with each application being certified, with the variations being in numbers of entries and the complexities of each.

The example used is a fairly simple application which is generally described on Worksheet 1. It consists of five functional security requirements, each followed by its security feature specifications, security tests and results, and finally an evaluation of the results.

The case is fictitious. The details of the specifications and tests are equally fictitious, relating to no particular hardware or situation. There was no intention to include an exhaustive set of requirements or tests, but only to show the reader how the finished certification worksheets might appear.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

1

(APPLICATION DESCRIPTION)

SYSTEM/APPLICATION TITLE		SVSISD		
DIVISION TIME-KEEPING SYSTEM (DTKS)		dtks.01	—	—
FUNC. CONTACT:	Perry Annum, Div. Scty., Tel: 5-7392	TECH. CONTACT	Meg O. Byte, DP Branch, Tel: 5-2937	
BRIEF FUNCTIONAL DESCRIPTION:				
<p>In order to improve the accuracy and timeliness of employee time-keeping for payroll purposes, the division implemented a PC based system under the primary operation and control of the division secretary, with the administrative assistant as alternate.</p> <p>Each day branch chiefs submit time slips to the division secretary for the previous duty day. The secretary enters the data into the appropriate employee records maintained on a PC. Each Monday at two week intervals, the secretary completes the entries for the previous Friday, copies the data onto a floppy disk and delivers it to the Payroll Office where it is entered into the Departmental Payroll System for processing.</p> <p>Since the data is entered very close to the source, the data error rate has decreased from 9.23% to .3%. The timeliness of the weekly input has become a non-problem since the workload is spread evenly over the pay period. And finally, the Payroll Office has reduced the Data Entry Section from the original 5 people to the present 2 people who are still required for other data entry tasks.</p>				
USER ENVIRONMENT				
<p>The software for this application has been implemented on the PC in the divisional office. This PC is one node of the division-wide local area network. There is concern about the possibility of someone making unauthorized changes to the records; accessing information protected by the Privacy Act; or destruction of the files, software, or ability to process which could seriously delay the payroll since that office no longer has the capability to handle the required level of data entry.</p>				
REASON FOR SENSITIVITY:				
<input checked="" type="checkbox"/>	STATUTE (LIST):	Privacy Act		
<input type="checkbox"/>	POLICY (SOURCE):			
<input checked="" type="checkbox"/>	CRITICAL TO (AGENCY & DEPT.):	Advanced Techniques Division		
<input type="checkbox"/>	OTHER (EXPLAIN):			

SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(FUNCTIONAL SECURITY REQUIREMENT)

SYSTEM/APPLICATION TITLE	STSSID	FUNC. ACNT.		
	dtks.01	1		
DESCRIPTION OF FUNCTIONAL SECURITY REQUIREMENT				
<p>Data storage media must be protected from theft, destruction, or unauthorized use.</p>				
REQUIRED EVIDENCE OF ADEQUACY				
<p>Data storage media are accessible only to the secretary and the administrative assistant.</p>				

SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(SECURITY FEATURE SPECIFICATIONS)

3

SYSTEM/APPLICATION TITLE	SYNID	FUNC. SCMT.	
	DTKS.01	1	—

DESCRIPTION OF SECURITY FEATURE

Develop and implement procedures to:

1. Store and maintain data on "floppy disk" only.
2. Complete the external label in accord with current policies and procedures and indicate that the disk contains sensitive information.
3. Keep data storage media (floppy) in a secure, locked container at all times except when it is being used by the division secretary or administrative assistant. When updating or use has been completed, the disk is to be returned to the locked container.
4. Access to the locked container must be limited to the two authorized individuals.
5. Upon departure or reassignment of one or both of the authorized persons, the combination or lock to the secure container will be changed.

DESIGN REVIEW

APPROVED

— CONDITIONALLY APPROVED (Explanation)

— DISAPPROVED (Explanation)

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

(SECURITY TESTS)

SYSTEM/APPLICATION NAME	TEST ID	FUNC. NAME	TEST #
DIVISION TIME-KEEPING SYSTEM (DTKS)		disk.01	1
TEST SCENARIO	TEST RESULTS		
<p>1. Determine that formal (written) procedures exist, are enforced, and specify as a minimum the security features listed on Worksheet 3 for this requirement.</p> <p>2. Check that execution of this application requires insertion of the properly labelled floppy disk containing the data file.</p> <p>3. After execution of application, terminate the job, remove the floppy, and again attempt execution. Application should not execute.</p> <p>4. Was the floppy disk obtained from a securely locked container?</p> <p>5. Was the person who opened the container one of the two persons authorized to do so?</p> <p>6. If the container has a combination lock, is there an external label listing the persons having access to the container?</p>	<p>1. Written procedures exist and incorporate the security features listed in Worksheet 3.</p> <p>2. Application would not execute until the data file on disk was inserted.</p> <p>3. Application would not execute without inserting the disk file.</p> <p>4. Data file disk was obtained from safe and returned there after use.</p> <p>5. An authorized person retrieved the disk.</p> <p>6. Safe has an external label listing persons having combination.</p>		

SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(SECURITY TESTS)

SYSTEM/APPLICATION NAME	SYNTH	FUNC. POW. +	TEST +
DIVISION TIME-KEEPING SYSTEM (DTKS)	dike.01	1	
TEST SCENARIO	TEST RESULTS		

7. Does the list contain names of persons other than the division secretary and administrative assistant?
8. Is there a record showing the last date of change of the lock or combination?
9. Have the incumbents of the authorized positions changed since the lock or combination was last changed?
10. What is your assessment of the security awareness and knowledge of the division secretary and administrative assistant?
7. Only the two authorized names were on the safe access list.
8. Safe access list indicates date of last combination change.
9. Incumbency of the two authorized positions have not changed since the date of last combination change.
10. Two authorized people are very security conscious and are thoroughly aware of the security policies and procedures.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET (EVALUATION)

SYSTEM/APPLICATION TITLE	SYSID	FUNC. REQ'D.	TEST
	dtks.01	1	

EVALUATION OF TEST RESULTS

Tests to evaluate the existence and effectiveness of controls or safeguards implemented to satisfy these functional security requirements were executed satisfactorily. Office security, given the security features of the surrounding area, are believed to be adequate from a procedural point of view.

The individuals occupying this office, both of whom have authorized access to the 'dtks' system, were involved in preparing the security features which were then reviewed by the System Security Officer and approved by the Division Chief. There appears to be a high state of security awareness and close adherence to security procedures.

RECOMMENDATIONS

Overall results of these tests satisfy the requirements listed in Functional Requirement #1. RECOMMEND CERTIFICATION OF THIS REQUIREMENT.

2

**SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(FUNCTIONAL SECURITY REQUIREMENT)**

SYSTEM/APPLICATION TITLE	SYSID	FUNC. REQMT. #	
	dtks.01	2	—

DESCRIPTION OF FUNCTIONAL SECURITY REQUIREMENT

The data lost, destroyed or damaged by any cause must be recoverable up to the end of the previous week.

REQUIRED EVIDENCE OF ADEQUACY

Demonstrate that data can be quickly and completely recovered up to and including the previous Friday.

5

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

(SECURITY FEATURE SPECIFICATIONS)

SYSTEM/APPLICATION TITLE	SYSID	FUNC. RQMT. #
	dtks.01	
DIVISION TIME-KEEPING SYSTEM (DTKS)	2	—

DESCRIPTION OF SECURITY FEATURE

Formal procedures will be prepared and implemented to:

1. Copy the information stored on the current floppy disk to another floppy disk at the end of each reporting week.
2. Insert the disk copy into the PC and access records near the beginning, middle, and end of the file to provide assurance that the file was copied completely.
3. Complete the external copy label in accord with current policies and procedures, indicating that the disk contains sensitive information.
4. Deliver the copy to a pre-determined off-site location which can provide storage security equal to or better than the primary location, and is sufficiently separated from the primary site that a single emergency is unlikely to damage or destroy both sites.
5. Copy to be delivered to the secure off-site location must be hand-carried by one of the two authorized persons, a bonded courier, or otherwise prepared and transported in accord with the departmental procedures for transmitting sensitive information.
6. Return the previously stored copy of the disk for re-use within the dtks.01 application only, taking care that it continues to receive the same protection as the current data file.

DESIGN REVIEW

APPROVED

— CONDITIONALLY APPROVED (Explain)

— DISAPPROVED (Explain)

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

4

(SECURITY TESTS)

SYSTEM/APPLICATION NAME	STORY	FUNC. NAME.	TEST
DIVISION TIME-KEEPING SYSTEM (OTKS)	date.01	2	
TEST SCENARIO	TEST ANSWERS		

1. Do formal procedures exist, and are they enforced to satisfy, at a minimum, the security features described on Worksheet 3 for this requirement?

2. Do the two authorized persons have an adequate knowledge of the procedures and the reasons for them?

3. Does the off-site storage location offer security adequate for the sensitivity of the data?

4. Is the off-site storage location sufficiently separated from the primary site to minimize the likelihood of both being effected by the same emergency?

5. At the off-site location, check to see if the file for the last reporting week is stored and properly labelled.

6. Are any earlier versions of the file in storage?

1. Formal, written security procedures exist and cover requirements listed on Worksheet 3.

2. Two authorized persons assisted in the writing of these procedures and are well acquainted with the procedures and the reasons for them.

3. Off-site storage site was visited and has security adequate for the sensitivity of the data.

4. Off-site storage site is approximately 5 miles from the primary site.

5. Off-site storage site contained the properly labelled backup files for the last cycle.

6. Only the most current files were in storage.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

4

(SECURITY TESTS)

SENSITIVE APPLICATION SITE	TEST SCENARIO	TEST RESULTS	FUNCTIONAL REQUIREMENT	TEST ID
DIVISION TIME-KEEPING SYSTEM (DTS)				

7. If yes, why?

8. How are the files delivered to and from the off-site storage location?
9. Determine if the files returned from the off-site storage location are afforded adequate protection en route and at the primary site.
7. If yes, why?
7. Not applicable.
8. Properly packaged and labelled backup files are delivered to the site by internal messenger.
9. Obsolete backup files are returned and stored in the safe until re-used.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

(EVALUATION)

5

SYSTEM/APPLICATION TITLE	SYSID	FUNC. ROUT. #	TEST #
	dtks.01	2	

EVALUATION OF TEST RESULTS

Tests were devised to verify the existence and effectiveness of the controls and safeguards to provide protection specified in Functional Requirement #2.

Formal backup and recovery procedures exist and appear to be followed.

Test team followed a floppy disk data file destined for the off-site storage location, looking for vulnerabilities which could be exploited. Based upon the perceived relatively low attractiveness of the data base, implemented precautions appear to be adequate.

The off-site storage location was visited and appropriate tests performed at that location. The site is sufficiently distant from the primary site so that it is unlikely to be effected by the same emergency as the primary site, except for major, wide-spread damage which could be caused by an earthquake or very large hurricane.

Data stored in the off-site location was checked to insure that only the latest file was stored. The previous version is returned to the primary site for re-use. The off-site storage location is operated by an organization dedicated to providing this service. Their procedures and security are adequate for date of a greater sensitivity than the DTKS. Pick-up and delivery of data files is accomplished by the site operator's bonded courier.

RECOMMENDATIONS

Tests indicate that Functional Requirements #2 were met.
RECOMMEND CERTIFICATION OF THIS REQUIREMENT.

2

**SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(FUNCTIONAL SECURITY REQUIREMENT)**

SYSTEM/APPLICATION TITLE	SYSID	FUNC. RQMT. #	
	dtks.01	3	_____

DESCRIPTION OF FUNCTIONAL SECURITY REQUIREMENT

Application software must be protected from unauthorized changes, damage, or destruction.

REQUIRED EVIDENCE OF ADEQUACY

Software can be accessed and executed only by the division secretary or administrative assistant, and changed only by the Technical Contact.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

(SECURITY FEATURE SPECIFICATIONS)

SYSTEM/APPLICATION TITLE	SYSID	FUNC. REQ'D.	
	dtks.01	3	—

DESCRIPTION OF SECURITY FEATURE

Software controls will be implemented to insure that the following restrictions are enforced:

1. The software based access control system cannot be by-passed.

2. The applications software will be stored on a floppy disk and loaded into the system for each execution cycle.

3. The applications software file will be afforded the same protection as that described for Functional Requirement #1.

4. Application software access and change privileges will be limited to the Technical Point of Contact entering the correct USERID and Password.

5. Application software execution privileges will be limited to the division secretary and administrative assistant, after entering the correct USERID and Password.

6. Record the USERID, date, and time (if possible) of all changes, or attempted changes, to the application software.

7. Logically dis-connect the PC being used after three unsuccessful attempts to change the application software.

8. Produce, on demand but under the control of the Systems Security Officer (USERID and password), a record of all successful or unsuccessful attempts to change the software, to include the USERID, date: and, if possible on the PC, the time of the attempt or access.

The software package known to provide these capabilities (and intended to be used), is the "SAVWARE" system.

DESIGN REVIEW


APPROVED

— CONDITIONALLY APPROVED (Request)

— DISAPPROVED (Request)

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

4

(SECURITY TESTS)

SYSTEM/APPLICATION NAME	ORG#	FUNC. ROM#	TEST #
DIVISION TIME-KEEPING SYSTEM (DTKS)		dtks.01	3
TEST SCENARIO	TEST RESULTS		
<p>1. LOGON another PC, executing a legitimate application, while the DTKS is being executed. Try to "crash" your application and, if successful, attempt a follow-on entry into the DTKS.</p> <p>2. Attempt a normal entry to the DTKS while it is being executed.</p> <p>3. Insure that applications software is stored on a floppy disk and must be loaded for each execution.</p> <p>4. After logging on to an authorized application, execute the following utilities in an attempt to by-pass the access control system:</p> <ul style="list-style-type: none"> a. Execute utility HEILIST. <p>Was the password file identified?</p> <p>b. Execute HEILIST 'password' word'. Was the password file accessed and the contents listed in clear text?</p> <p>c. Execute HEICOPY (dtks.01).</p> <p>Was the time-keeping file listed?</p>	<p>1. Attempted several times to access the division office PC before and after "crashes" but could not penetrate.</p> <p>2. Unable to enter dtkns normally from another PC while it was operating.</p> <p>3. Application requires loading software for each execution.</p> <p>4a. Identified password file name by using HEILIST.</p> <p>4b. Executed HEILIST 'password' and contents were listed in clear text.</p> <p>4c. Executed HEICOPY and time-keeping file was not listed.</p>		

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

4

(SECURITY TESTS)

SYSTEM/APPLICATION NAME	FUNCTIONALITY	TEST SCENARIO					
DIVISION TIME-KEEPING SYSTEM (DTKS)	<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>STAFF</td> <td>FUNC. NO.1.</td> <td>TEST 1</td> </tr> <tr> <td>dtks.01</td> <td>3</td> <td></td> </tr> </table> TEST RESULTS:	STAFF	FUNC. NO.1.	TEST 1	dtks.01	3	
STAFF	FUNC. NO.1.	TEST 1					
dtks.01	3						

5. List the dtk8 Privilege Table to determine:

- a. That only the division secretary and administrative assistant have execution privilege for the application software.
- b. That only these two individuals have access and change privileges for the dtk8 file.
- c. That only the Technical Contact has access and change privileges for the application software.
- d. That privileges not specifically granted are specifically denied.

5. Listed the dtks Privilege Table:

- 5a. Only division secretary and administrative assistant have execution privileges.
- 5b. Only these two persons can change the privilege table.
- 5c. The dtks Privilege Table gives the technical contact the capability to access and change the application software.
- 5d. No other privileges for the software.
- 6. With help of technical contact, made changes to the application software and check to see if an audit trail has been created.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

4

(SECURITY TESTS)

SYSTEM/APPLICATION TITLE	TEST ID	FUNC. NO.1.	TEST 2.
DIVISION TIME-KEEPING SYSTEM (DTKS)	dtks.01	3	
TEST SCENARIO			TEST RESULTS

7. Attempt unauthorized changes to the application software and check to see that an audit trail has been created.

8. Make four unsuccessful attempts to change the application software to see if the PC used is "locked out" after the third attempt.

9. Use several different and illegal USERIDs to see if the application can be accessed.

10. Use a valid UserID but several different passwords to determine the response of the system.

11. Using the UserID and password of the System Security Officer, produce a listing of the audit trail and ascertain if all successful or unsuccessful software changes, and all unsuccessful attempts to access the application have been recorded.

7. Made several attempts to access and make unauthorized changes to the software, without success. These attempts were adequately recorded in the audit trail.

8. Verified that the system locks out the PC after three unsuccessful attempts to change software.

9. Had several authorized users of the local area network attempt to logon to the dtks, without success.

10. Used authorized UserID and made 18 unsuccessful attempts to guess the correct password from known personal data for the two authorized persons.

11. System Security Officer produced a listing of the audit trail which was compared with each of the test steps. All pertinent information had been recorded.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

(EVALUATION)

5

SYSTEM/APPLICATION TITLE	SYSID	FUNC. RQMT. #	TEST #
	dtks.01	3	

EVALUATION OF TEST RESULTS

Generally, Functional Security Requirements #3 were satisfied by the implemented controls and safeguards tested. There were, however, two notable exceptions:

1. Certain high level, vendor supplied utilities have the capability to unnecessarily expose certain data. Although these utilities are not normally used by the applications staff, they are available for use. (See test step 4a and 4b).

2. Test step 4b revealed that the 'password' file was stored and could be listed in clear text. Although it is likely that only the systems programmers would be using these utilities they do not, and should not, be able to read the password file.

Recommend conditional certification of the controls and safeguards designed to satisfy Functional Requirement #3. To meet these conditions requires the following:

1. High-level utilities having the potential capability to circumvent security controls should be placed in a separate data set and protected by passwords known only to the systems programming staff, unless impelling reasons dictate otherwise.

2. New passwords being entered into the password file should go through a "one-way" encryption algorithm---cannot be decrypted. User passwords entered through a terminal or PC should then undergo the same one-way encryption before comparing with the password file.

2

**SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(FUNCTIONAL SECURITY REQUIREMENT)**

SYSTEM/APPLICATION TITLE	SYSTID	FUNC. RQMT. #	
DIVISION TIME-KEEPING SYSTEM (DTKS)	dtks.01	4	—

DESCRIPTION OF FUNCTIONAL SECURITY REQUIREMENT

Only the division secretary or administrative assistant can access or alter the data file.

REQUIRED EVIDENCE OF ADEQUACY

Proof that these privileges are limited to these two individuals.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(SECURITY FEATURE SPECIFICATIONS)

3

SYSTEM/APPLICATION TITLE	STUDIO	FUNC. RQMT. #	
	dtks.01	4	—

DESCRIPTION OF SECURITY FEATURE

The software package mentioned in Func. Rqmt. #3 will be used to:

1. Maintain the data file on the "floppy disk" as specified in Functional Requirement # 1.
2. Provide file access and updating privileges only to the two authorized individuals based upon their USERID and password.
3. Deny all privileges not specifically granted.
4. Logically dis-able any PC originating three consecutive unsuccessful attempts to access the file.
5. When not in actual use, the data storage media will be protected as described in Functional Requirement # 1.

DESIGN REVIEW

APPROVED

— CONDITIONALLY APPROVED (Capital)

— DISAPPROVED (Capital)

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

4

(SECURITY TESTS)

SYSTEM/APPLICATION NAME	TEST SCENARIO	TEST ID	FUNC. NOV. #	TEST #
DIVISION TIME-KEEPING SYSTEM (DTKS)		dtks.01	4	

1. Load the dtks.01 application software and attempt execution without inserting the floppy disk data file.

2. Check Privilege Table to see if the file can be accessed and/or changed only by the division secretary or administrative assistant.

3. Check table to determine if all privileges not specifically authorized are specifically denied.

4. Make four unsuccessful attempts to access the data file. PC should be disabled after third unsuccessful attempt. Required action by operations staff to enable PC.

5. When not in use, is the floppy data file stored in the approved locked container?

1. Loaded application and attempted execution. Would not execute without also loading the data file.
2. Listed privilege table for data file. The only two entries are for the authorized persons who have access and change capabilities.

3. All other privileges are "turned-off".
4. Made four unsuccessful attempts to access the data file. PC was disabled after the third unsuccessful attempt. Required action by operations staff to enable PC.

5. Upon termination of an authorized session, the screen instructs user to remove floppy disk data file and return to the safe.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET (EVALUATION)

5

SYSTEM/APPLICATION TITLE	STUDIO	FUNC. RQMT.	TEST
DIVISION TIME-KEEPING SYSTEM (DTKS)	dtks.01	4	

EVALUATION OF TEST RESULTS

Tests executed to verify the existence and effectiveness of the controls and safeguards to satisfy Functional Requirement #4 were satisfactory.

RECOMMENDATIONS

RECOMMEND CERTIFICATION OF THE CONTROLS AND SAFEGUARDS EXTANT TO SATISFY FUNCTIONAL SECURITY REQUIREMENTS # 4.

2

**SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(FUNCTIONAL SECURITY REQUIREMENT)**

SYSTEM/APPLICATION TITLE	SYSPID	FUNC. RQMT. #	
DIVISION TIME-KEEPING SYSTEM (DTKS)	dtks.01	5	_____

DESCRIPTION OF FUNCTIONAL SECURITY REQUIREMENT

PC is protected from theft or mis-use.

REQUIRED EVIDENCE OF ADEQUACY

Demonstrate ability to limit use of the PC to the division secretary and administrative assistant only.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET
(SECURITY FEATURE SPECIFICATIONS)

3

SYSTEM/APPLICATION TITLE	SYSID	FUNC. ROMT. #	
	dtks.01	6	—

DESCRIPTION OF SECURITY FEATURE

Physical security features will be installed and/or implemented as follows:

1. PC in divisional office will be securely anchored to a desk or equally large piece of furniture.
2. A key lock will be installed to interrupt main power to the PC whenever the lock is activated.
3. The activating key will be kept in the locked container where the data storage media is secured in order to remain under the control of the division secretary or administrative assistant at all times.
4. The physical dis-connection of main power (disconnecting the wall plug) will cause an alarm to be sounded at the guard post.

DESIGN REVIEW

APPROVED

— CONDITIONALLY APPROVED (Explain)

— DISAPPROVED (Explain)

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

4

(SECURITY TESTS)

SYSTEM/APPLICATION TITLE	TEST SCENARIO	TEST RESULTS
DIVISION TIME-KEEPING SYSTEM (DTS)		

1. Is the PC securely fastened to a large piece of furniture with a locking device?

2. A key lock is installed on the PC to interrupt the main power when the lock is activated.

3. The main power interrupt lock is activated at the close of business.

4. The key to the power interrupt switch is secured along with the floppy disk data file.

5. Dis-connect power at the wall outlet:
a. Did alarm sound at the guard station?

b. Do guard force written procedures cover the actions expected of them?

1. PC is secured to the desk by the Anchor Pad locking device.
 2. Key lock interrupts the main power when the lock is activated.
 3. Key lock is activated whenever PC is not in use.
 4. The key is kept in the safe along with the data and software floppies.
 5. Wall plug to PC was removed:
- 5a. Verified that alarm sounded at guard desk and indicated location of problem.
- 5b. Verified that written guard procedures provide adequate instructions for the guards.

SENSITIVE APPLICATION CERTIFICATION WORKSHEET

4

(SECURITY TESTS)

SYSTEM/APPLICATION TITLE DIVISION TIME-KEEPING SYSTEM (DTKS)	TEST SCENARIO	TEST RESULTS	TEST NUMBER & DATE
	<p>c. Did guard force respond promptly?</p> <p>d. Did guard force know what to do?</p> <p>5c. Guard arrived at site within two minutes.</p> <p>5d. Guard ascertained that persons present were authorized to be within the area. Was then told that this was a security test. When questioned, was very familiar with the procedures for such a situation.</p>		

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4451
2. PERFORMING ORGANIZATION REPORT NUMBER

4. TITLE AND SUBTITLE

U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications

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 20889

7. CONTRACT/GANT 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 Commerce, Office of Information Resources Management, Washington, DC 20230

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)

The Methodology for Certifying Sensitive Computer Applications defines and describes a standard certification methodology employed by the U.S. Department of Commerce to a) ensure that sensitive applications meet applicable federal policies, regulations, and standards and b) demonstrate that installed security safeguards are adequate for the sensitivity or criticality of the data processed, as required by OMB Circular A-130. This methodology takes the reader through the certification process step-by-step, including determining whether an application requires certification, defining functional security requirements, defining system security specifications, reviewing system security features design, testing those features, accepting the test results for a certification decision, and the final decision to implement and operate the application. The document also describes how audits, internal control reviews and risk analyses fit into the certification process.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

ADP security, application security, automated information systems security, computer application certification, computer application, computer security, software security

13. AVAILABILITY

UNLIMITED

FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE,
WASHINGTON, DC 20402.

X ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES

107

15. PRICE

A06

