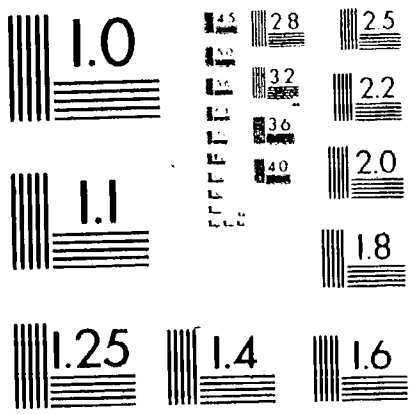
PG



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS
STANDARD REFERENCE MATERIAL 1010a
(ANSI and ISO TEST CHART No. 2)

DOCUMENT RESUME

ED 247 897 IR 011 246

AUTHOR Ruthberg, Zella G.; Neugent, William
TITLE Overview of Computer Security Certification and Accreditation. Final Report..
INSTITUTION National Bureau of Standards (DOC), Washington, D.C. Inst. for Computer Sciences and Technology.
REPORT NO NBS-SP-500-109
PUB DATE Apr 84
CONTRACT NB80SBCA0323
NOTE 27p.
AVAILABLE FROM Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.
PUB TYPE Guides - General (050) -- Reports - Descriptive (141)

EDRS PRICE MF01/PC02 Plus Postage.
DESCRIPTORS *Administrative Organization; Certification; *Computers; Guidelines; Management Information Systems; *Program Development; *Program Evaluation; *Program Implementation; Standards; Systems Development
IDENTIFIERS *Computer Security

ABSTRACT

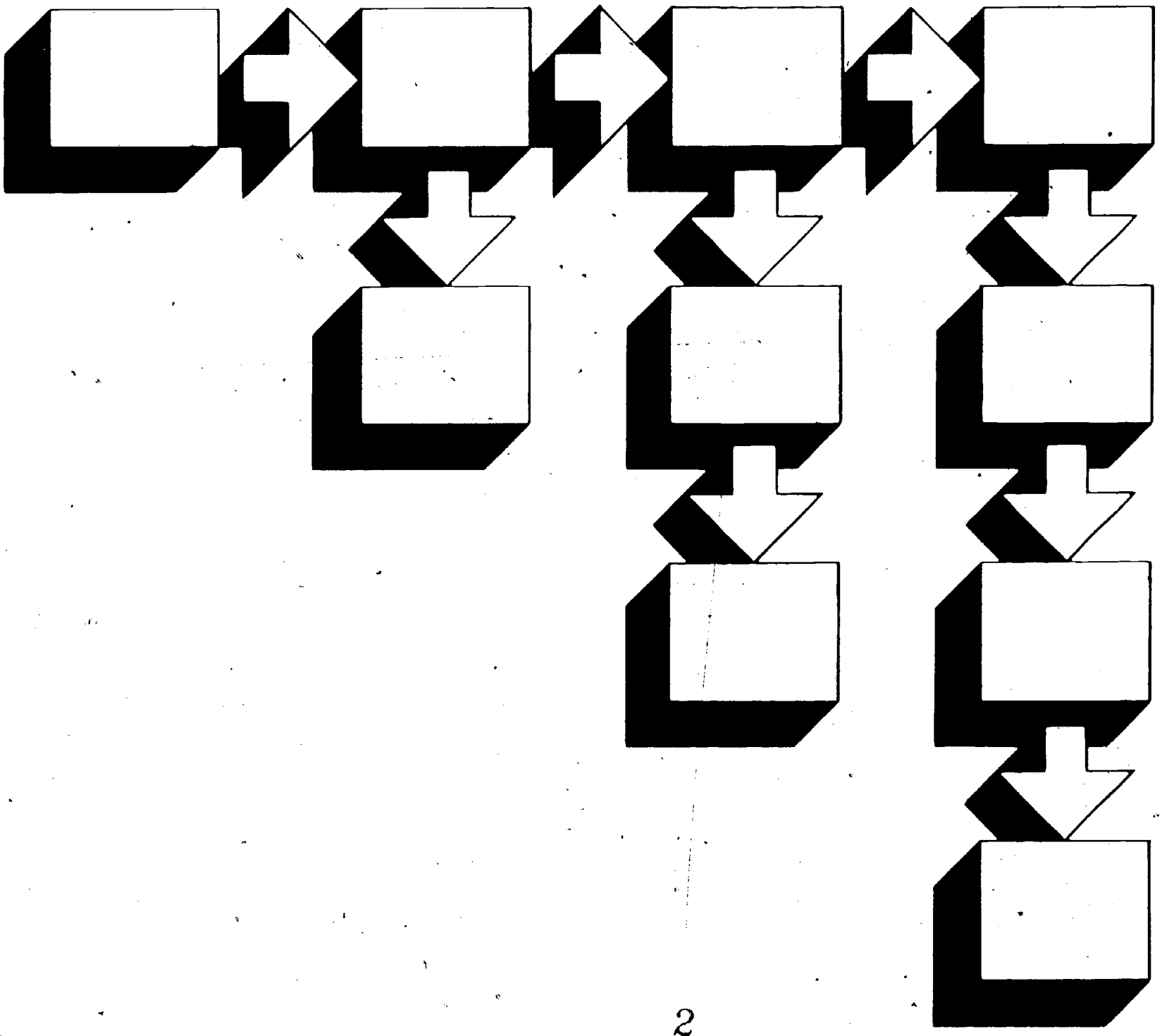
Primarily intended to familiarize ADP (automatic data processing) policy and information resource managers with the approach to computer security certification and accreditation found in "Guideline to Computer Security Certification and Accreditation," Federal Information Processing Standards Publications (FIPS-PUB) 102, this overview summarizes an approach to developing a program and performing a technical process for certification and accreditation of sensitive computer applications. The steps involved in the process are briefly identified and described, as are program management issues and the principal functional roles needed within an organization to carry out such a program. Recertification and reaccreditation and their relation to change control are also touched upon. A discussion of evaluation techniques to be used for certification includes risk analysis, EDP audit (a subdivision of internal audit), VV&T (verification, validation, and testing), and security safeguard reviews. The relation of these techniques to the system lifecycle is indicated. (Author/LMM)

U.S. Department of Commerce
National Bureau of Standards

Computer Science and Technology

NBS Special Publication 500-109

Overview of Computer Security Certification and Accreditation



NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards[1] was established by an act of Congress on March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, and the Institute for Computer Sciences and Technology.

THE NATIONAL MEASUREMENT LABORATORY provides the national system of physical and chemical and materials measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; conducts materials research leading to improved methods of measurement, standards, and data on the properties of materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; develops, produces, and distributes Standard Reference Materials; and provides calibration services. The Laboratory consists of the following centers:

Absolute Physical Quantities[2] — Radiation Research — Chemical Physics — Analytical Chemistry — Materials Science

THE NATIONAL ENGINEERING LABORATORY provides technology and technical services to the public and private sectors to address national needs and to solve national problems; conducts research in engineering and applied science in support of these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the ultimate user. The Laboratory consists of the following centers:

Applied Mathematics — Electronics and Electrical Engineering[2] — Manufacturing Engineering — Building Technology — Fire Research — Chemical Engineering[2]

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Institute consists of the following centers:

Programming Science and Technology — Computer Systems Engineering.

[1] Headquarters and Laboratories at Gaithersburg, MD, unless otherwise noted; mailing address Washington, DC 20234.
[2] Some divisions within the center are located at Boulder, CO 80303.

Computer Science and Technology

NBS Special Publication 500-109

Overview of Computer Security Certification and Accreditation

Zella G. Ruthberg

Center for Programming Science and Technology
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, DC 20234

William Neugent

System Development Corporation
7929 Westpark Drive
McLean, VA 22102

U.S. DEPARTMENT OF COMMERCE
Malcolm Baldrige, Secretary

National Bureau of Standards
Ernest Ambler, Director

Issued April 1984

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

Library of Congress Catalog Card Number: 84-601002

National Bureau of Standards Special Publication 500-109
Natl. Bur. Stand. (U.S.), Spec. Publ. 500-109, 23 pages (Apr. 1984)
CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1984

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

FOREWORD

This overview is intended to provide ADP policy managers, information resource managers, ADP technical managers, and ADP staff with a comprehensive summary of and guide to FIPS PUB 102, "Guideline to Computer Security Certification and Accreditation," September 27, 1983. FIPS PUB 102 presents in detail an approach to developing a program and performing a technical process for certifying and accrediting sensitive applications. By summarizing FIPS PUB 102 and referencing its relevant sections, this overview will not only enable its different type audiences to obtain a complete picture of the certification/accreditation activity, but also direct these audiences to parts of FIPS PUB 102 relevant to them. This overview and FIPS PUB 102 should be of particular interest to all those responsible for responding to Office of Management and Budget Circular A-71, Transmittal Memorandum Number 1, July 27, 1978.

CONTENTS

		Page
SECTION 1	INTRODUCTION	1
1.1	PROBLEMS ADDRESSED	1
1.2	CONTEXT FOR COMPUTER SECURITY CERTIFICATION AND ACCREDITATION	2
1.3	ENTITIES REQUIRING CERTIFICATION AND ACCREDITATION	2
SECTION 2	WHAT ARE CERTIFICATION AND ACCREDITATION?	4
2.1	CERTIFICATION PROCESS	4
2.1.1	Planning (Sec. 2.1)	5
2.1.2	Data Collection (Sec. 2.2)	6
2.1.3	Basic Evaluation (Sec. 2.3)	6
2.1.4	Detailed Evaluation (Sec. 2.4)	9
2.1.5	Report Of Findings (Sec. 2.5)	10
2.2	ACCREDITATION (SEC. 2.6)	11
2.3	RECERTIFICATION AND REACCREDITATION (SEC. 2.7)	12
2.4	EVALUATION TECHNIQUES FOR SECURITY CERTIFICATION (SEC. 1.5)	12
2.4.1	RISK ANALYSIS	12
2.4.2	VALIDATION, VERIFICATION, AND TESTING (VV&T)	13
2.4.3	SECURITY SAFEGUARD EVALUATION	13
2.4.4	EDP AUDIT	13
SECTION 3	ESTABLISHING A PROGRAM (SEC. 1 AND 3)	15
3.1	POLICIES AND PROCEDURES (SEC. 3.1)	15
3.2	ROLES AND RESPONSIBILITIES	15
3.3	ORGANIZATION STRUCTURE CONCERNS (SEC. 3.2)	16
3.4	SCHEDULING (SEC. 1.4)	16
3.5	STAFFING, TRAINING, AND SUPPORT (SEC. 3.3)	16

FIGURES

Figure 1	The Certification Process	4
Figure 2	Life Cycle Phases and Security Processes	14

---

[1] Section numbers in parentheses indicate where this material may be found in FIPS PUB 102, "Guideline for Computer Security Certification and Accreditation," September 27, 1983.

SECTION 1

INTRODUCTION

Some computer security risks threaten the very existence of an organization. Critical decisions regarding the adequacy of security safeguards in sensitive applications must be made by authorized managers and must be based on reliable technical information. Certification gives managers this technical information and accreditation gives them the structure needed to make such critical decisions. Together they provide management a quality control technique for computer security. They help managers protect against fraud, illegal practices, mission failures, embarrassing 'leaks'" and legal action, and help keep them from being 'surprised' by problems within their computer systems. This Guideline explains the need for and describes the major features of the certification and accreditation processes.

1.1 PROBLEMS ADDRESSED

Although the introduction of computers into the daily operation of organizations has sometimes obscured the issue, managers are still responsible for protecting the organization's vital resources, including its information systems. Computers affect this security responsibility in two important ways. First, computers can radically change information system vulnerabilities from those found in manual systems and, in many cases, can increase the risks to data and resources. Second, computers increase the complexity of systems, thus making such systems more difficult to understand and protect. Safeguards can be much more complex than those used in manual systems, and the evaluation of these also becomes more complex. Some examples of the changes introduced by computers and the security problems raised by these changes are:

1. Data assets can be more centralized, thus permitting larger scale frauds and magnifying errors.

2. Decisions formerly made by people can be made automatically, making such decisions more susceptible to tampering.

3. Access may be achieved electronically through a remote terminal, rather than directly at the computer site, thus permitting unauthorized and unobserved access more readily.

4. Duties previously separated for security reasons may be integrated in the computer, thus allowing frauds and errors to occur undetected.

5. The computer can become such a critical asset that its failure may cause major organizational disruption.

6. Organizations' management structures are shifting to accommodate computer technology. This often results in fuzzy allocation of management responsibility, creating holes and overlaps in management control.

To counter these problems, managers need techniques to assess and cost-effectively improve their computer security posture. Certification and accreditation, when applied to computer security, are techniques for achieving these ends.

1.2 CONTEXT FOR COMPUTER SECURITY CERTIFICATION AND ACCREDITATION

Computer security certification and accreditation are only one aspect of a general certification and accreditation activity that should be performed to ensure that a computer application satisfies its defined functional, performance, security, and quality requirements. This general process often utilizes the same methods, techniques, and technical tools used for performing technical evaluations for other purposes. The guidance here focuses on those aspects of this general process that are relevant to the computer security of an ADP application. For the remainder of this overview 'computer security certification,' 'security certification,' and 'certification' will be used synonymously as will the terms 'computer security accreditation,''security accreditation,' and "accreditation."

1.3 ENTITIES REQUIRING CERTIFICATION AND ACCREDITATION

Certification and accreditation are only performed on those applications sensitive enough to warrant such attention, where an application's sensitivity derives from the potential loss or harm associated with a security failure during operation (Sec. 1.2.7)[1]. To be cost-effective, this process also requires that an organization form a prioritized list of sensitive applications, based on factors such as mission importance, asset value, and anticipated threats. Some organizations have sensitivity categorization schemes which they

---

[1] Section numbers in parentheses indicate where this material may be found in FIPS PUB 102, "Guideline for Computer Security Certification and Accreditation."

use for this prioritizing activity (App. C).

In this discussion 'computer system' and 'computer application' are closely related terms. A computer system is an assembly of elements including at least hardware and usually also software, data, procedures, and people, so related as to behave as an interacting or interdependent unity (Sec. 1.2.4); a computer application is the use(s) for which a computer system is intentionally employed (Sec. 1.2.5).

SECTION 2

WHAT ARE CERTIFICATION AND ACCREDITATION?

Certification is the technical evaluation of compliance with security requirements for the purpose of accreditation. The technical evaluation uses a combination of security evaluation techniques described later and culminates in a technical judgment of the extent to which safeguards meet security requirements. Accreditation is official authorization for operation (or, in cases of security deficiencies, for security corrections or suspension of certain activities). (Sec. 1.2.2 and 1.2.3)

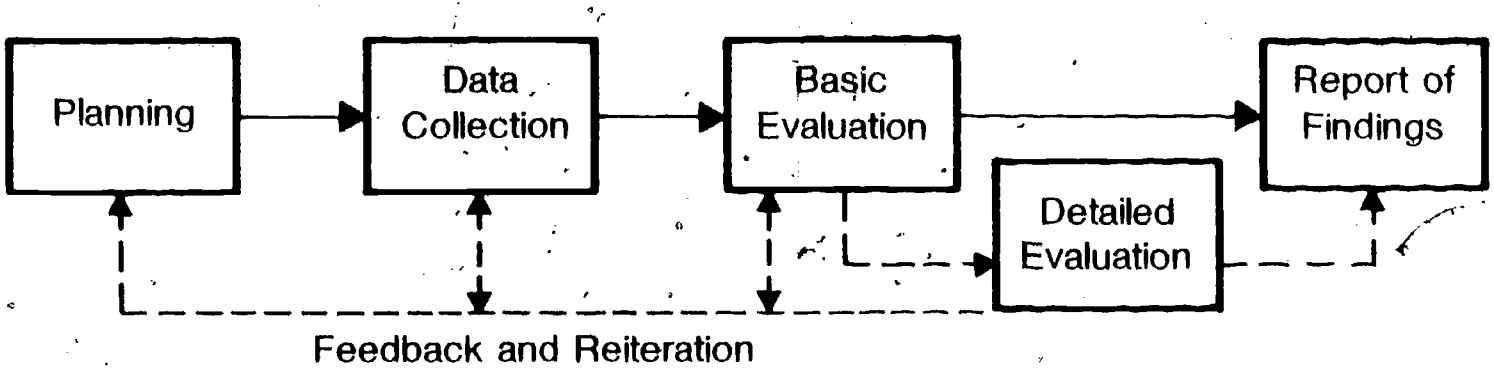


Figure 1. The Certification Process

2.1 CERTIFICATION PROCESS

Figure 1 summarizes the certification process. It is iterative in that, based on findings from each stage, previous stages might have to be reentered and work performed again. Typically most or all of the stages are ongoing at the same time. The intent of the figure is to show the shift in emphasis as work progresses.

There are two levels of activity associated with security evaluation for certification: basic evaluation and detailed evaluation. Basic evaluation means 'high-level' or 'overview-type' evaluation and is essential in all certifications. Usually basic evaluation suffices for most aspects of an application under review. However, most certifications also require detailed work in problem areas and therefore require some detailed evaluation as well.

Time and resources required to perform a certification vary widely from case to case. If potential loss or harm is low, certification cost must also be kept low. Risk analysis can help in deciding how much certification review is cost justified. Resources for certification may vary from several person-days to many person-months. Minimum products required from certification and accreditation are a security evaluation report and an accreditation statement.

The certification process described here is in a functional form. It tells what must be done and presents a general functional view of how to accomplish it. Detailed specifics of security evaluation for certification will differ widely from case to case and must be adapted to meet specific application needs. Aids such as detailed evaluation methods and checklists are helpful in the adaptation process but no single detailed method exists that can be used universally.

Since the certification process described is at a functional level, it can be applied to both applications under development and those already operational. For example, both could include review of similar documentation such as Functional Requirements Documents and test procedure reports. Detailed evaluation methods differ for the two situations, however, due to differences in the types of data available, the time frame in which data are available, and the organization of the work.

2.1.1 Planning (Sec. 2.1)

Since the planning process must anticipate problem areas and define needs for specialized skills, it requires that the planners perform a very high-level quick review of the entire application in order to gain an understanding of the issues involved. Additional planning tasks are those of (1) placing boundaries on the effort, (2) partitioning the work, (3) identifying areas of emphasis, and (4) drawing up a certification plan.

For certification, application boundaries must be drawn to include all relevant facets of the application's environment including the administrative, physical, and technical areas. Without this comprehensive review, certification gives an incomplete and perhaps misleading picture of application security. For example, excellent technical controls may be rendered worthless if administrative security duties are not properly defined.

Within these overall boundaries, certification work is usually partitioned based on the specialized skills involved. A sample partitioning of security evaluation responsibility areas follows: administrative security, computer operation, contingency planning, change control, data entry and output, operating system, communication security, personnel security, physical security, environmental controls, development method, application software controls, data base management system, and hardware.

The greatest emphasis should be placed on areas of greatest potential loss or harm. These may have been identified in an earlier risk analysis or in reports of past problems or violations. It may also be that the accrediting official(s), based on management judgment, desire emphasis in a particular area.

The information collected in the planning phase forms the basis for the application's certification plan (Sec. 2.1.4). Suggested sections for the plan include security requirements, the evaluation approach, the evaluation team make-up, a schedule, required support, and evaluation products.

2.1.2 Data Collection (Sec. 2.2)

The ideal source of information is application documentation. Critical documents are (1) application system security requirements; (2) a risk analysis showing threats and assets; (3) an application flow diagram showing inputs, processing steps, and outputs, along with complete transaction flows for important transaction types; and (4) a listing of application controls. Unfortunately, few applications have a complete set of this documentation. Where such documents do not exist, the most efficient technique for gathering this information is for application personnel to prepare this documentation and to also provide supplementary tutorial briefings to the certification team. Document reviews of the more commonly found documents (e.g., user manuals) and interviews are also needed to expand upon and corroborate the information in the documents listed above.

2.1.3 Basic Evaluation (Sec. 2.3)

Basic evaluation is primarily concerned with the overall security function posture. For example, it might be concerned with whether authorization subjects must include terminals as well as individuals and processes.

There are four tasks in a basic evaluation:

1. Security Requirements Evaluation (are security requirements acceptable?)

2. Security Function Evaluation (does the design or description of security functions satisfy the security requirements?)

3. Control Implementation Determination (are the security functions implemented?)

4. Methodology Review (does the implementation method provide assurance that security functions are acceptably implemented?)

1. Requirements Evaluation: Requirements evaluation is important because certification is only meaningful if the application has well-defined security requirements. Unfortunately this is often not the case. This task then critically examines any documentation of these requirements and compares it with Federal, state, organizational and user requirements. Where no such documentation exists, the security requirements implied in the application must be formulated.

In both formulating and evaluating security requirements, consideration is given to Federal and state laws and regulations, organizational standards and policies, and the specific application needs. The four primary areas considered in defining application needs are assets, exposures, threats, and controls. Corresponding questions to be answered are: What should be protected? What might happen to assets if a threat is realized? What are assets being protected against? and How effective are security safeguards in reducing exposures?

If a risk analysis has been performed for the application or its environment, many situational security needs might already be well defined. Other useful tools are computer security checklists and questionnaires, many of which are now available [2].

2. Function Evaluation: Function evaluation determines whether security functions such as authentication, authorization, monitoring, security management, and security labeling satisfy security requirements. With well-defined security requirements, this function evaluation becomes the most important task in basic evaluation. The primary method is to use the stated requirements as a checklist. For example, where called for in requirements: Is individual accountability provided? Are subjects and objects identified and given security labels? Is an execute-only mode of access provided? Are all file accesses recorded? Are functions partitioned so as to provide separation of duties? Does a contingency plan exist and has it been tested?

---

[2] For further information see Ruthberg, Zella G. (Editor), William Neugent, John Gilligan, and Lance Hoffman, "Technology Assessment: Methods for Measuring the Level of Computer Security," NBS Special Publication _, (currently in draft-Sept. 1981).

An important concern for function evaluation is the appropriate level of detail. The recommendation is that basic evaluations be complete (for all applicable control features) down through the functional specification level, as defined in (or appropriate for definition in) the Functional Requirements Document. This notion applies to both controls within the computer and physical/administrative controls external to it (although the latter might not actually be defined in a Functional Requirements Document).

This function evaluation approach is suggested in full realization of the difficulties confronted in determining which functions to include in a Functional Requirements Document, and, when this document is incomplete or non-existent, in examining other sources of application information (e.g., operating procedures, specifications). The reasons are that the functional specification level (1) is a legitimate, commonly-used level, and (2) represents a complete picture of security functions and services with respect to the environment surrounding the application. Completeness is necessary to ensure that major problem areas are not overlooked.

3. Control Implementation Determination: The fact that functions are described in a document or discussed in an interview does not prove that they have been implemented. The existence of most physical and administrative controls can be determined via visual inspection. For controls internal to the computer, testing is needed. In many cases, a short operational demonstration suffices. For example, the existence of a password function can be determined by attempting to use the application and verifying that a valid password is required. Black box (external) testing is generally sufficient for control implementation determination.

4. Methodology Review: It is desirable to gain some assurance that controls are acceptably implemented. The best way to do this without becoming immersed in extensive testing or detailed analysis is to examine the methodology used to develop the application. This step applies regardless of whether the application is currently under development or has long been operational.

Methodology review contributes to a confidence judgment on the extent to which controls are reliably implemented and on the susceptibility of the application to flaws. If review findings suggest that the implementation cannot be relied upon, detailed evaluation is required in order to find specific flaws. Specific flaws are far preferable as certification evidence than a general judgment of low confidence.

Areas of concern in reviewing an application development methodology for certification are summarized below. Several of the areas also apply to security products obtained from vendors.

1. Documentation. Is there current, complete, and acceptable quality documentation? This applies to both developmental and operational documentation.

2. Objectives. Was security explicitly stated and treated as an objective? Were security requirements defined?

3. Project Control. Was development well controlled? Were independent reviews and testing performed and did they consider security? Was an effective change control program used?

4. Tools and Techniques. Were structured design techniques used (e.g., modularization, formal specifications)? Were established programming practices and standards used (e.g., high order languages, structured walk-throughs)?

5. Resources. How experienced were the people involved? What were the sensitivity levels or clearances associated with their positions?

2.1.4 Detailed Evaluation (Sec. 2.4)

In many cases a basic evaluation does not provide sufficient evidence for certification. Examples are cases where (1) basic evaluation reveals problems that require further analysis, (2) the application has a high degree of sensitivity, or (3) primary safeguards are embodied in detailed internal functions that are not visible or suitable for examination at the basic evaluation level. These situations require detailed evaluations to obtain additional evidence and increased confidence in evaluation judgments.

Detailed evaluations analyze the quality of security safeguards. Primary tasks are the examination of the application from three possible points of view and the use of any of several techniques for detailed focusing:

1. Functional Operation (Do controls function properly?)

2. Performance (Do controls satisfy performance criteria?)

3. Penetration Resistance (How readily can controls be broken or circumvented?)

4. Detailed Focusing (What security components need detailed analysis? What really happens in the detailed processing of a transaction?)

The tasks in detailed evaluation are performed as needed. Testing is the most common technique used. Other validation and verification techniques are also available and are becoming more widely used.

1. Functional Operation: This point of view is most often emphasized, since it assesses protection against human error and casual attempts at abuse. Tests of functional operation examine areas

such as control operation, parameter checking, common error conditions, control monitoring, and control management. Software tools for program analysis and formal verification methods are applicable.

2. Performance: There is much more to the quality of safeguards than proper functional operation. Performance factors relevant to security include availability, survivability, accuracy, response time, and throughput. Stress testing is a useful evaluation technique.

3. Penetration Resistance: Penetration resistance evaluation can be used to establish confidence in security safeguards. It can also find and correct flaws, although recent history has shown the inadequacy of 'find and fix' as an approach for achieving security. Since penetration resistance evaluation is different in kind from other forms of evaluation, it can at times play a useful role in certification.

4. Detailed Focusing: It is rarely feasible or desirable to examine everything in detail. In addition to evaluation from some or all of the points of view discussed above, two other strategies are especially useful for focusing on narrow portions of the security picture: one based on security components and one based on situational analysis.

Security-relevant components upon which attention might be focused are assets, exposures, threats, and controls. Examples of possible types of analysis include asset value, asset exploitation, exposure impact, perpetrator, control, work-factor, and safeguard tradeoff. It is difficult to anticipate precise needs for such studies when planning certification, although it is safe to assume that some will be needed.

Situational analysis addresses the problem of application complexity, which limits not only the percentage of the application that can be examined, but also the degree of understanding attainable for those portions that are examined. Two useful forms of it are (1) the analysis of attack scenarios and (2) the analysis of transaction flows. Both can be used to complement the high-level completeness of basic evaluation by providing detailed, well-understood examples.

2.1.5 Report Of Findings (Sec. 2.5)

The security evaluation report is the primary product of certification. It contains technical and management security recommendations and is the primary basis for the accreditation decision. The report should:

1. Summarize the security standards or policies that were applied.

2. Summarize the controls that are in place.

3. Summarize major vulnerabilities, recommending which should be corrected and which should be left as residual.

4. Recommend and prioritize corrective actions, if warranted, along with anticipated costs and impacts. Recommend operational restrictions where necessary.

5. Summarize the certification process, so the accreditor(s) can determine how much confidence to place in the findings.

6. Include a proposed accreditation statement (which might be positive or negative).

The certification process should produce the security evaluation report plus other documentation that can be used to support the findings and to evaluate the certification process itself.

2.2 ACCREDITATION (SEC. 2.6)

The accreditor(s) is(are) responsible for evaluating the certification evidence, deciding on the acceptibility of application security safeguards, approving corrective actions, ensuring that corrective actions are accomplished, and issuing the accreditation statement. Aids to be used to assist in this process include answers to questions on resources used (how much, who), processes used (review mechanisms, coordination of findings), and report content (reasonableness, support of findings). Accreditation responsibilities must be integrated into the normal decision-making process of the organization.

Since applications that warrant certification and accreditation are usually important to organization operations, most flaws will not be severe enough to remove an operational application from service. There are many intermediate accreditation alternatives available. The most common is to withhold accreditation pending completion of corrections. Many types of operational restrictions are also possible. For example:

1. Adding procedural security controls. Restricting use of the application to sites that have compensating controls.

2. Restricting the application to process only nonsensitive or minimally sensitive data.

3. Removing especially vulnerable application functions or components. In a network environment a particularly weak node might be excluded from the network.

4. Restricting users to only those with approved access to all data being processed or to those who have passed a background investigation. Restricting use of the application to non-critical situations where errors or failures are less severe.

5. Removing remote access (thus relying more on physical security).

6. Granting conditional accreditation for a 'shakedown' period before added trust is granted.

2.3 RECERTIFICATION AND REACCREDITATION (SEC. 2.7)

Once an application has been initially certified (whether during development or after becoming operational), the work is not over. As an application or its security environment changes, recertification and reaccreditation are needed.

It is not practical for the accreditor(s), who might be a senior official or a committee of officials, to personally approve every change. On the other hand, substantive changes do require reaccreditation. This gives rise to a need for levels of recertification and reaccreditation based on levels of change. The three levels suggested are: (1) major, affecting the basic security design; (2) intermediate, affecting two or more security software modules or a major hardware component; and (3) minor, within one security software module. The elements of the certification process and the organizational placement of the accreditor differ for each level, with more extensive changes requiring both more extensive evaluation and higher placement of reaccreditation responsibility.

Change control (configuration management) can provide an important assist to recertification and reaccreditation since it is required during both development and operation. Every change should be reviewed for its impact on prior certification evidence.

2.4 EVALUATION TECHNIQUES FOR SECURITY CERTIFICATION (SEC. 1.5)

For certification and accreditation to be used properly, it is essential to know what evaluation techniques are available and when to apply them. There are four groups of techniques currently used in security evaluation that can be used for certification, either alone or in combination. They differ from one another in their purpose and/or in the organizational entities that use them. The four groupings of methods are: (1) risk analysis, (2) validation, verification, and testing, (3) security safeguard evaluation, and (4) EDP audit. (See Figure 2 for their relation to life cycle phases.)

2.4.1 RISK ANALYSIS

The primary purpose of risk analysis is to understand the security problem by identifying security risks, determining their magnitude, and identifying areas where safeguards are needed. It can also be used to determine how many resources to budget for security and where to allocate these resources. It can be performed at the

beginning of the application life cycle and, with user inputs and policy requirements, can provide the basis for application security requirements. When performed later in the application life cycle, it is useful for evaluating security when reliable data exist on threats (e.g., occurrences of fires and floods). Under these conditions, the evaluation may be used for security certification. Risk analysis is usually performed under the direction of people internal to the application in question. (Sec. 1.5.1)

2.4.2 VALIDATION, VERIFICATION, AND TESTING (VV&T)

VV&T is a process of review, analysis, and testing that should be performed on an application throughout its life cycle but is particularly cost effective when performed during the early life cycle. Validation determines the correctness of the application with respect to its requirements; verification checks the internal consistency and completeness of the application as it evolves and passes through different levels of specification; and testing, either automated or manual, examines application behavior by exercising it on sample data sets. The performance of VV&T provides a powerful quality assurance technique for applications, and when requirements include security, VV&T becomes an important evaluation technique for security certification. VV&T is usually performed by the people responsible for developing the application; however, for critical applications it may be done by an independent body. (Sec. 1.5.2)

2.4.3 SECURITY SAFEGUARD EVALUATION

Security safeguard evaluation methods are primarily concerned with assessing the security solution. They can be thought of as a specialized form of VV&T. They involve validating security requirements, examining safeguards, and determining whether safeguards satisfy security requirements. Numerous methods are being used for this type evaluation (i.e., checklists, control matrices, weighted ratings for levels of security produced by controls). It can be the major contributor to evaluations for certification. It is typically performed by people independent of the application in question but internal to the organizational division within which the application resides. A security officer may head such an evaluation. (Sec. 1.5.3)

2.4.4 EDP AUDIT

EDP audit, a subdivision of internal audit, assesses controls against control objectives in agency applications that rely on computers. It is usually broader in scope than just the consideration of security issues. Like security safeguard evaluation, it assesses compliance with policies, existence of controls, and adequacy of controls, but EDP audit might also address cost and efficiency in meeting mission objectives. When control objectives for security are considered, EDP audit becomes a form of certification evaluation. Unlike security safeguard evaluation, however, EDP audit is an

activity external to the organizational division in which the application resides and is used by higher-level managers to manage the organization. (Sec. 1.5.4)

Life Cycle Phase	Security Concern	Preferred Security Process to be Applied
I. INITIATION	A. Understand the security problem: identify security risks; determine their magnitude; identify areas where safeguards are needed.	_____ Risk Analysis
	B. Define security requirements.	
II. DEVELOPMENT DEFINITION DESIGN PROGRAMMING TESTING	A. Validate security requirements.	_____ Risk Analysis, VV&T
	B. Assess recommended and implemented safeguards; determine whether they satisfy requirements.	_____ Certification
	C. Approve for operation.	_____ Accreditation
III. OPERATION AND MAINTENANCE	A. Reassess security risks.	_____ Risk Analysis Safeguard Eval. EDP Audit
	B. Reassess safeguards.	_____ Recertification*
	C. Approve for continued operation.	_____ Reaccreditation

*If risk analysis, VV&T, certification and accreditation were not performed during development, they might be performed initially during operation. It is far preferable to perform them during development, however.

Figure 2. Life Cycle Phases and Security Processes

SECTION 3

ESTABLISHING A PROGRAM (SEC. 1 AND 3)

In order to establish a certification and accreditation program in an organization, five issues must be considered in addition to the issue of application sensitivity.

1. Policy and procedures authorizing and defining the program,
2. Roles and responsibilities defining who does what,
3. Organization structure concerns that influence the program,
4. Scheduling when things are done,
5. Staffing, training and support needs.

3.1 POLICIES AND PROCEDURES (SEC. 3.1)

Policies and procedures should be incorporated in (1) a Program Directive that establishes official authority for the program, issuing from the Senior Executive Officer and (2) a Program Manual defining the processes involved, issuing from the Certification Program Manager. The Program Directive could be part of the directive establishing the overall agency security program and should contain a program summary (including purpose) as well as the delegation of major responsibilities. The Program Manual should reflect the responsibilities of the Certification Program Manager and could use the Guideline (FIPS PUB 102) structure as the basis for such a manual.

3.2 ROLES AND RESPONSIBILITIES

The most important consideration in defining responsibilities is proper selection of the accrediting authority (Accrediting Official(s), Sec. 1.3.1). This might be a high-level manager or a group of officials who are responsible for the system and who have authority to remedy deficiencies. Certification personnel are primarily technical (Security Evaluator, Sec. 1.3.4), although every

certification effort requires a manager (Application Certification Manager, Sec. 1.3.3). Also, the organization might have a central coordinator or director for all certification activities (Certification Program Manager, Sec. 1.3.2). In some cases several certification efforts are performed in support of one accreditation decision. It is preferable to integrate such multiple technical certification findings into one final report.

3.3 ORGANIZATION STRUCTURE CONCERNS (SEC. 3.2)

Although there is no universally applicable way to structure the organization of a certification and accreditation program, there are two universal concerns in this area: (1) the need for an appropriate high-level manager as Accrediting Official and (2) the need for Security Evaluators who are as objective as possible. (A sample organization structure is shown in Appendix G.)

3.4 SCHEDULING (SEC. 1.4)

The next issue is when this combined certification and accreditation process is performed. It begins with requirements definition and continues through development, operation, and maintenance of an application. It must be integrated into the life cycle management process. Also, it is far preferable to initially certify and accredit an application under development than after it has become operational. The primary reason is that an application under development is easier to change. A second reason is that certification during development permits the development process itself to be improved.

3.5 STAFFING, TRAINING, AND SUPPORT (SEC. 3.3)

In order for the staffing, training, and support for certifications to be adequate, there is a serious need for management wihin agencies to consider the importance of computer security in general to the proper operation of their computer applications. Sufficient attention must be given to both career paths for security staff and the proper training of such persons in security evaluation. Funding commensurate with the sensitivity of the applications involved should be allocated for such staffing and training as well as for general administrative support.

Two further points are noteworthy concerning technical support. First, it is often best to use both independent and internal people for security evaluation. Independent people provide necessary objectivity, although they are costly since outsiders must take the time to learn details of the application. Internal people are typically less costly, and can benefit greatly from the computer security training and increased security awareness they gain from participation, but are usually less objective. The second point is that certification can make much use of validation, verification, and

testing findings and of reviews that are routinely performed during development and operation. It is not practical for certification to duplicate these activities. On the other hand, it is desirable for certification needs to influence them, (e.g., by anticipating and recording these needs in VV&T planning).

NBS-114A (REV. 2-8C)

U.S. DEPT. OF COMM. **BIBLIOGRAPHIC DATA SHEET** *(See instructions)*	1. PUBLICATION OR REPORT NO. NBS SP 500-109	2. Performing Organ. Report No.	3. Publication Date April 1984

4. TITLE AND SUBTITLE

Computer Science and Technology:

Overview of Computer Security Certification and Accreditation

5. AUTHOR(S)

Zella G. Ruthberg and William Neugent

6. PERFORMING ORGANIZATION *(If joint or other than NBS, see instructions)*

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

System Development Corp.
7929 Westpark Drive
McLean, VA 22102

7. Contract/Grant No.
NB80SBCA0323

8. Type of Report & Period Covered
Final January 1981-
September 1982

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS *(Street, City, State, ZIP)*

National Bureau of Standards
Washington, DC 20234

10. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 84-601002

[ ] Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)*

This overview is primarily intended for use by ADP policy managers and information resource managers to become familiar with the approach to computer security certification and accreditation found in "Guideline for Computer Security Certification and Accreditation," FIPS PUB 102. ADP technical managers and staff will also find it a useful overview. This overview summarizes how to establish and carry out a program and a technical process for computer security certification and accreditation of sensitive computer applications. The overview identifies and briefly describes the steps involved in performing computer security certification and accreditation; it identifies and briefly discusses important issues in managing a computer security certification and accreditation program; and it identifies and briefly describes the principal functional roles needed within an organization to carry out such a program. Recertification and reaccreditation and its relation to change control are also touched upon. A discussion of evaluation techniques to be used for certification includes risk analysis, EDP audit, VV&T (verification, validation, and testing), and security safeguard reviews. The relation of these to the system lifecycle is indicated.

12. KEY WORDS *(Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)*

accreditation; certification; certification/accreditation management; certification/accreditation process; certification/accreditation program; computer security evaluation; EDP audit; recertification/reaccreditation; risk analysis; sensitive computer application; sensitivity classification; verification, validation, and testing (VV&T).

13. AVAILABILITY

[X] Unlimited

[ ] For Official Distribution. Do Not Release to NTIS

[X] Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

[ ] Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES
23

15. Price

USCOMM-DC 6043-P80

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SCIENCE & TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Bureau of Standards Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. As a special service to subscribers each issue contains complete citations to all recent Bureau publications in both NBS and non-NBS media. Issued six times a year. Annual subscription: domestic $18; foreign $22.50. Single copy, $5.50 domestic; $6.90 foreign.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NBS under the authority of the National Standard Data Act (Public Law 90-396).

NOTE: The principal publication outlet for the foregoing data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NBS publications—FIPS and NBSIR's—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.