NCSC-TG-029

Library No. S-239,954

Version 1

FOREWORD

The National Computer Security Center is publishing Introduction to Certification and Accreditation as part of the "Rainbow Series" of documents our Technical Guidelines Program produces. This document initiates a subseries on certification and accreditation (C&A) guidance, and provides an introduction to C&A including an introductory discussion of some basic concepts related to C&A, and sets the baseline for future documents on the same subject. It is not intended as a comprehensive tutorial or manual on the broad topic of information systems security. It should be viewed, instead, as guidance in meeting requirements for certification and accreditation of automated information systems.

The combination of the information age, technology, and national policy, has irrevocably pushed us into an Information Systems Security age. The explosion in the uses of telecommunication devices and automated information systems has resulted in a corresponding explosion in opportunities for unauthorized exploitation of valuable information. The technology necessary to perform this exploitation is available not only to our foreign adversaries but also to criminal elements.

As the Director of the National Computer Security Center, I invite your suggestions for revising this document. We plan to review and revise this document as the need arises. Please address all proposals for revision through appropriate channels to:

National Computer Security Center

9800 Savage Road

Ft. George G. Meade, MD 20755-6000

Attention: Chief, Standards, Criteria, and Guidelines Division

January 1994

Patrick R. Gallagher, Jr.

Director

National Computer Security Center

ACKNOWLEDGMENTS

This document has been produced under the guidance of U.S. Navy Lieutenant Commander Candice A. Stark. This version of the document was developed with the assistance of many organizations, in addition to the NSA groups, and include: Aerospace Corp.; Beta Analytics, Inc; Boeing Aerospace Co.; Booz, Allen and Hamilton; Bureau of the Census; Central Intelligence Agency; Computers & Security; Computer Sciences Corp.; CTA, Inc.; Cybercom Research Corp.; Defense Intelligence Agency; Defense Logistics Agency; Defense Mapping Agency; Defense Nuclear Agency; Department of Justice; Defense Information Systems Agency; Drug Enforcement Administration; Dynetics Inc; Gemini Computers, Inc.; Grumman Data Systems; General Services Administration; GTE; Harris Corp. ESD; Honeywell Federal Systems; ITT Research Institute; Information Security International, Inc.; Internal Revenue Service; Joint Chiefs of Staff; Lesnett and Associates, Inc; Lockheed; Locus, Inc; Los Alamos National Laboratories; Martin Marietta Defense Space and Communications; MITRE Corp; NASA AIS Security Engineering Team; National Defense University; National Institute of Standards and Technology; Office of the Secretary of Defense; On-Site Inspection Agency; Robert M. Wainwright & Assoc; RCAS; SAIC Communication Systems; Seidcon & Company; Space Application Corp.; Suffern Associates; Trusted Information Systems; TRW; U.S. Air Force; U.S. Army, U.S. Navy, U.S. Marine Corps; University of Southern California Information Sciences Institute. Individuals in these organizations gave generously of their time and expertise in the useful review and critique of this document.

ABSTRACT

This document, which provides an introduction to certification and accreditation (C&A) concepts, provides an introductory discussion of some basic concepts related to C&A and sets the baseline for further documents. Its objectives are the following: (1) to provide an overview of C&A, its function and place within the risk management process; (2) to clarify the critical roles the Designated Approving Authority (DAA) and other key security officials must assume throughout the C&A process; (3) to identify some of the current security policies, emphasizing some key policy issue areas; and (4) to define C&A-related terms. The details of the actual C&A process are not included in this document, but will be provided in a follow-on document(s).

Suggested Keywords: certification, accreditation, Designated Approving Authority (DAA),
INFOSEC, security policy

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SECTION 1

INTRODUCTION

1.1 Background

In recent years, there has been a shift in perspective of information systems security (INFOSEC) from viewing it as a number of independent, loosely coupled disciplines to a more cohesive, interdependent collection of security solutions. The current environment of declining resources and the rapid advances in technology have demanded changes in assessing the security posture of systems and implementing an INFOSEC systems engineering process. These changes are necessary to reduce fragmentation and to ensure and maintain consistency and compatibility among all aspects of the security of a system. In addition, the dynamic threat environment necessitates a more efficient, integrated view of INFOSEC disciplines.

In considering the overall security of a system, two essential concepts are (1) that the (security) goals of the system be clearly stated and (2) that an analysis be made of the ability of the system to (a) satisfy the original goals and (b) continue to provide the attributes and security required in the evolving environment. The Department of Defense (DoD) and other federal agencies have formalized these concepts. DoD policy states that any automated information system (AIS) that processes classified, sensitive unclassified, or unclassified information must undergo a technical analysis and management approval before it is allowed to operate [1]. The technical analysis establishes the extent to which the system meets a set of specified security requirements for its mission and operational environment. The management approval is the formal acceptance of responsibility for operating at a given level of risk. The technical analysis and management approval processes are called certification and accreditation (C&A), respectively. These concepts, however, are quite general and can be applied with different levels of formality and within different organizational structures.

One of the most important tasks required to provide an integrated, cost-effective

information
systems security program, is to develop uniform certification and accreditation guidance. The use
of AISs within all aspects of operations, the dynamic organization of systems, and the exchange of
information among systems point to the need for uniform guidance when certifying and accrediting
systems. The National Security Agency (NSA), in support of its mission to provide guidelines on
the acquisition, certification, accreditation, and operation of systems, plans to publish a series of
documents focusing on these issues. This introductory document discusses the basic concept of
C&A of systems in an effort to provide improvements in the secure development, operation, and
maintenance of systems.

1.2 Scope

This document provides an overview to some basic concepts and policies of C&A. Individuals
serving as system accreditors, system certifiers, program managers (PMs), developers, system
integrators, system engineers, security officers, evaluators, and System users will benefit from this
document by gaining a basic understanding of C&A. People in each of the many roles involved in
C&A will have a different focus and emphasis on related activities. Therefore, it is important that
everyone involved has a basic understanding of the high-level process and uses common
terminology. This document provides a basic overview of C&A, but it is not a replacement for
reviewing and understanding the specific national, federal, department, and service/agency
policies and guidelines in the actual performance of C&A.

The concepts of C&A presented in this document apply to all types of systems: existing and
proposed systems, stand-alone systems, personal computers (PCs), microcomputers,
minicomputers, mainframes, large central processing facilities, networks, distributed systems,
embedded systems, workstations, telecommunications systems, systems composed of both
evaluated and unevaluated components, other security components, and systems composed of
previously accredited systems (particularly when some of these accredited systems have not been
certified or have been certified against differing criteria). Guidance on applying the high-level
C&A process to particular types of systems, as well as associated activities, will be provided in
subsequent documents in this series.

1.3 Purpose

The purpose of this C&A concepts document is to discuss the high-level C&A process, authority
for C&A, C&A policy, and C&A terminology. This document sets the baseline for a series of

documents and has the following objectives:

· Discuss the high-level C&A process and its relationship to risk management and INFOSEC disciplines.

· Clarify the critical roles the DAA and key security officials must assume throughout the C&A process.

· Identify several current security policies, emphasizing areas that are ambiguous or not addressed in current policy.

· Define basic C&A terms.

1.4 Evaluation Versus Certification

Evaluation is a term used in many different ways causing much confusion in the security community. Sometimes it is used in the general English sense meaning judgment or determination of worth or quality. Based on common usage of the term in the security community, one can distinguish between two types of evaluations: (1) evaluations that exclude the environment, and (2) evaluations that include the environment. This second type of evaluation, meaning an evaluation conducted to assess a systems security attributes with respect to a specific operational requirement(s), is what this series of documents refers to as certification. Evaluations that exclude the environment are analysis against a standard or criteria. There are a number of examples of this type of evaluation:

· Commercial off-the-shelf (COTS) products evaluated against the Trusted Computer System Evaluation Criteria (TCSEC) (Orange Book) [2] or the Canadian or European Criteria

· Compartmented Mode Workstations (CMW) evaluated against the Compartmented Mode Workstation Evaluation Criteria, Version 1 (CMWEC) [3] and the TCSEC

· Communications products with embedded communications security (COMSEC) components evaluated against the FSRS (NSA Specification for General Functional Security Requirements for a Telecommunications System (FSRS) [4])

· Products evaluated against the TEMPEST criteria (DoD Directive (DoDD) C-5200.19 [5])

Products that have been evaluated against the FSRS and that satisfactorily meet the minimum requirements (and are successfully considered for NSA approval) are generally said to be endorsed products. Products evaluated against the TCSEC are often referred to as evaluated products. While current usage of these terms varies widely, in this document, the term evaluation will refer to a

security analysis of a component against a given set of standards or criteria without regard to the environment, while certification refers to a security analysis of a system against a given set of security requirements in a given environment.

SECTION 2

OVERVIEW OF C&A

Certification and accreditation constitute a set of procedures and judgments leading to a determination of the suitability of the system in question to operate in the targeted operational environment.

Accreditation is the official management authorization to operate a system. The accreditation normally grants approval for the system to operate (a) in a particular security mode, (b) with a prescribed set of countermeasures (administrative, physical, personnel, COMSEC, emissions, and computer security (COMPUSEC) controls), (c) against a defined threat and with stated vulnerabilities and countermeasures, (d) within a given operational concept and environment, (e) with stated interconnections to other systems, (f) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility, and (g) for a specified period of time. The Designated Approving Authority(s) (DAA) formally accepts security responsibility for the operation of the system and officially declares that the specified system will adequately protect against compromise, destruction, or unauthorized modification under stated parameters of the accreditation. The accreditation decision affixes security responsibility with the DAA and shows that due care has been taken for security in accordance with the applicable policies.

An accreditation decision is in effect after the issuance of a formal, dated statement of accreditation signed by the DAA, and remains in effect for the specified period of time (varies according to applicable policies). A system processing classified or sensitive unclassified information should be accredited prior to operation or testing with live data unless a written waiver is granted by the DAA. In some cases (e.g., when dealing with new technology, during a transition phase, or when additional time is needed for more rigorous testing), the DAA may grant an interim approval to operate for a specified period of time. At the end of the specified time period, the DAA must make the final accreditation decision.

Certification is conducted in support of the accreditation process. It is the comprehensive analysis of both the technical and nontechnical security features and other safeguards of a

system to
establish the extent to which a particular system meets the security requirements for its mission and
operational environment. A complete system certification must consider factors dealing with the
system in its unique environment, such as its proposed security mode of operation, specific users,
applications, data sensitivity, system configuration, site/facility location, and interconnections
with other systems. Certification should be done by personnel who are technically competent to
assess the systems ability to meet the security requirements according to an acceptable
methodology. The resulting documentation of the certification activities is provided to the DAA to
support the accreditation decision. Many security activities support certification, such as risk
analysis, security test and evaluation, and various types of evaluations.

Ideally, certification and accreditation procedures encompass the entire life cycle of the system.
Ideally, the DAA is involved from the inception of the system to ensure that the accreditation goals
are clearly defined. A successful certification effort implies that system security attributes were
measured and tested against the threats of the intended operational scenarios. Additionally,
certification and accreditation are seen as continuing and dynamic processes; the security state of
the system needs to be tracked and assessed through changes to the system and its operational
environment. Likewise, the management decision to accept the changing system for continued
operation is an ongoing decision process. The following sections provide a description of risk
management, the high-level C&A process, and recertification/reaccreditation.

2.1 Risk Management and C&A

Risk management is the total process of identifying, measuring, and minimizing uncertain events
affecting resources [1]. A fundamental aspect of risk management is the identification of the
security posture (i.e., threats and vulnerabilities) of the system, and stating the characteristics of
the operational environment from a security perspective. The primary objective of risk
management is to identify specific areas where safeguards are needed against deliberate or
inadvertent unauthorized disclosure, modification of information, denial of service, and
unauthorized use. Countermeasures can then be applied in those areas to eliminate or adequately
reduce the identified risk. The results of this activity provide critical information to making an
accreditation decision.

Risk management may include risk analysis, cost-benefit analysis, countermeasure selection,
security test and evaluation (ST&E), countermeasure implementation, penetration

testing, and
systems review. For DoD organizations, enclosure 3 to DoDD 5200.28 mandates a risk management program for each AIS to determine how much protection is required, how much
exists, and the most economical way of providing the needed protection. Other federal departments
and agencies have similar policy documents that should be referenced for guidance.

Risk analysis minimizes risk by specifying security measures commensurate with the relative
values of the resources to be protected, the vulnerabilities of those resources, and the identified
threats against them. Risk analysis should be applied iteratively during the system life cycle. When
applied to system design, a risk analysis aids in countermeasure specification. When applied during
the implementation phase or to an operational system, it can verify the effectiveness of existing
countermeasures and identify areas in which additional measures are needed to achieve the desired
level of security. There are numerous risk analysis methodologies and some automated tools
available to support them.

Management commitment to a comprehensive risk management program must be defined as early
as possible in the program life cycle. In scheduling risk management activities and designating
resources, careful consideration should be given to C&A goals and milestones. Associated risks
can then be assessed and corrective action considered for risks that are unacceptable.

2.2 C&A High-Level Process

The C&A process is a method for ensuring that an appropriate combination of security measures
are implemented to counter relevant threats and vulnerabilities. This high- level process consists
of several iterative, interdependent phases and steps illustrated in Figure 2.1. The scope and
specific activities of each step depend upon the system being certified and accredited (see section
2.2.2).

Step 1 of the C&A process focuses on identifying and assessing the specific security-relevant
aspects (i.e., tailoring factors) of a system. It involves gathering and developing relevant
documentation (e.g., policy implementation guidance, security regulations/manuals, previous
certification reports, product evaluation reports, COTS manuals, design documentation, design
modification, and security-related waivers). This identification provides the foundation for
subsequent phases, and is critical to determining the appropriate C&A tailoring guidance to be used
throughout the C&A process. Aspects to be considered include:

- Mission criticality

- Functional requirements
- System security boundary
- Security policies
- Security concept of operations (CONOPS)
- System components and their characteristics
- External interfaces and connection requirements
- Security mode of operation or overall risk index
- System and data ownership
- Threat information
- Identification of the DAA(s)

Step 2 involves C&A planning. Since security should have been considered with system conception, planning for C&A is a natural extension of system security planning. That is, the schedule (milestones) and resources (e.g., personnel, equipment, and training) required to complete the C&A process are identified. C&A planning information is incorporated into and maintained in program documentation. This information is also used to estimate the C&A budget.
Aspects to be considered in this step include:

- Reusability of previous evidence
- Life-cycle phase
- System milestones (time constraints)

Figure 2.1. High-Level C&A Process

Step 3 involves analyzing the security aspects of the system as a whole (i.e., how well security is employed throughout the system). During this phase, the certification team becomes more familiar with the security requirements and the security aspects of individual system components.
Specialized training on the specific system may be necessary depending upon the scope of this phase as well as the experience of the certification team. C&A activities include determining whether system security measures adequately satisfy applicable requirements. To accomplish this objective, security measures of the various disciplines are assessed and tested collectively.
Additionally, system vulnerabilities and residual risks are identified.

Step 4 involves documenting/coordinating the results and recommendations of

previous phases to prepare the certification package and accreditation package. The certification package is the consolidation of all the certification activity results. It will be used as supporting documentation for the accreditation decision, and will also support recertification/reaccreditation activities. The compilation of the supporting documentation should be done consistently and cost-effectively. The types of documentation generally included as part of the certification package include:

- System need/mission overview
- Security policy
- Security concept of operation or security plan
- System architectural description and configuration
- Reports of evaluated products from a recognized government evaluation (e.g., NSA product evaluation, the Defense Intelligence Agency (DIA)/NSA compartmented mode workstation (CMW) evaluation)
- Statements from other responsible agencies indicating that personnel, physical, COMSEC, or other security requirements have been met (e.g., Defense Message System (DMS) component approval process (CAP) functional testing)
- Risks and INFOSEC countermeasures (e.g., risk analysis report)
- Test plans, test procedures, and test results from security tests conducted (including penetration testing)
- Analytic results
- Configuration Management plan
- Previous C&A information
- Contingency plan

The accreditation package presents the DAA with a recommendation for an accreditation decision, a statement of residual risk, and supporting documentation which could be a subset of the certification package. It may be in the form of a technical document, technical letter, or annotated briefing. The information generally included as part of the accreditation package includes as a minimum:

- Executive summary of mission overview, architectural description, and system configuration, including interconnections
- Memorandum of Agreements (MOA)
- Waivers signed by the DAA that specific security requirements do not need to

be met or
are met by other means (e.g., procedures)

· Residual risk statement, including rationale for why residual risks should be accepted/
rejected

· Recommendation for accreditation decision

Step 5 is optional and involves the DAA(s) or his/her representative(s) conducting a site
accreditation survey to ensure the security requirements meet the requirements for the system.
Final testing can be conducted at this time to ensure the DAA(s) are satisfied that the residual risk
identified meets an acceptable level of risk to support its purpose. The activities include:

· Assess system information (this is the certification package review)

· Conduct site accreditation survey

Step 6 involves the DAA making the accreditation decision. This decision is based on many
factors, such as global threats, system need/criticality, certification results and recommendations,
residual risks, the availability or cost of alternative countermeasures, and factors that transcend
security such as program and schedule risks, and even political consequences. The DAA has a
range of options in making the accreditation decision, including the following:

· Full accreditation approval for its originally intended operational environment, including
a recertification/reaccreditation timeline

· Accreditation for operation outside of the originally intended environment (e.g., change
in mission, crisis situation, more restrictive operations)

· Interim (temporary) accreditation approval, identifying the steps to be completed prior to
full granting of accreditation and any additional controls (e.g., procedural or physical
controls, limiting the number of users) that must be in place to compensate for any increased risk

· Accreditation disapproval, including recommendations and timelines for correcting
specified deficiencies

Step 7 involves maintaining the system accreditation throughout the system life cycle.
Accreditation maintenance involves ensuring that the system continues to operate within the stated
parameters of the accreditation. For example, that the stated procedures and controls of the system
stay in place and are used, that the environment does not change outside of the stated parameters,
that other types of users are not added to the system (e.g., users with lower

clearances), that no additional external connections are made to the systems or that additional security requirements are not imposed on the system. Any substantial changes to the stated parameters of the accreditation may require that the system be recertified or reaccredited. It is important to note that recertification and reaccreditation activities may differ from those performed in support of a previous accreditation decision. For example, the system security mode of operation may change from system-high to compartmented mode, requiring more stringent security measures and an in-depth analysis of these measures. Applicable security policies/regulations, C&A team members, and/or DAA(s) may also change. Section 2.3 provides more information on events that affect system security that might require a system to be recertified or reaccredited.

2.2.1 Certification and Associated Security Disciplines

Certification activities and the associated results/recommendations are performed in support of the accreditation decision. Certification is a method for ensuring that an appropriate combination of system security measures are correctly implemented to counter relevant threats and vulnerabilities. That is, the certification effort must assess the effectiveness and interdependencies of security measures, as well as possible interferences or conflicts among them. These measures are typically based on the system security policy and operational requirements. It must be emphasized that in order to provide a realistic and effective analysis of the security posture of a system, all appropriate security disciplines (an INFOSEC perspective) must be included in the scope of the certification. For example, while a system may have very strong contro