NSTISSAM COMPUSEC/1-99
11 March 1999

ADVISORY MEMORANDUM ON THE TRANSITION FROM THE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA TO THE INTERNATIONAL COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY

National Security Telecommunications And Information Systems Security Committee

NATIONAL MANAGER

FOREWORD

1. This Advisory Memorandum provides guidance to U.S. Government Departments and Agencies regarding the transition from the Trusted Computer System Evaluation Criteria (TCSEC) (better known as the "Orange Book") to the International Common Criteria for Information Technology Security Evaluation Version 2.0 (hereinafter referred to as the "Common Criteria"). It is intended to introduce departments and agencies to the new criteria and provide an opportunity for them to evaluate its applicability to their Information Assurance (IA) operating environments and requirements. The Chairman of the Subcommittee on Information Systems Security will be accepting comments from members with the objective of promulgating the Common Criteria as a National Security Telecommunications and Information Systems Security Instruction within the next 6-12 months.

2. This Advisory Memorandum replaces, COMPUSEC 1-85, Subject: The Department of Defense Trusted Computer System Evaluation Criteria (U), dated 18 November 1985, which is hereby cancelled.

KENNETH A. MINIHAN
Lieutenant General, USAF

NSTISSC Secretariat (I42) • National Security Agency • 9800 Savage Road STE 6716 • Ft Meade MD 20755-6716
(410) 854-6805 • UFAX: (410) 854-6814
nstissc@radium.ncsc.mil

ADVISORY MEMORANDUM ON THE TRANSITION FROM THE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA TO THE INTERNATIONAL COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION

SECTION I - GENERAL BACKGROUND

1. Over the last decade, U.S. Government departments and agencies have made progress in strengthening the security of their information systems. The Trusted Computer System Evaluation Criteria (TCSEC) helped "set the bar" for security standards for operating systems and databases, and its corresponding evaluation program has issued compliance certificates for over one hundred commercial security-enabled products. The TCSEC "C2" level for operating system security has received worldwide acceptance and spawned similar security standards within Canada and the European Community.

2. Within the last several years, information assurance has evolved at a pace whereby it has become increasingly clear that the TSCEC is too rigid and limited in scope for many of today's security-enabled products and user application environments. As the state of the art for information assurance continues to evolve worldwide, it has become increasingly clear that updated criteria are required. Additionally, information security vendors have been pleading for internationally accepted criteria instead of individual nationally-based criteria which required their products be evaluated against a multitude of different standards depending on the region of the world where sales were being targeted.

3. Given these circumstances and recognitions, representatives from the National Security Agency (NSA) and the National Institute for Standards and Technology (NIST) joined with representatives from the governments of Canada, the United Kingdom, the Netherlands, France, and Germany, to draft a new international criteria for the specification and evaluation of information security technology. This new criteria, known as the Common Criteria, will be ratified in early 1999 by the International Standards Organization (ISO) as ISO 15408. In the United States, NIST and NSA have established the National Information Assurance Partnership (NIAP) to accredit private sector laboratories to evaluate products to this standard.

4. The Common Criteria differs from the TCSEC in its standardization approach. The TCSEC defined the specific security functionalities which must exist and the specific testing which must be performed to verify the security functionalities were implemented correctly (i.e. assurance) in predefined classes such as C2, B1 etc. Conversely, the Common Criteria is more of a lexicon or language which provides a standardized and comprehensive list of security functionalities and analysis techniques which may be performed to verify proper implementation, as well as a common evaluation methodology to perform the tests. The greater the degree of analysis, the higher the assurance that the product performs as advertised. It is up to the customer to select from these lists the security functionalities required in a specific product or application as well as the degree of evaluation to be performed. This is documented in a "Protection Profile." Thus, the TCSEC C2 class, for example, can be specified in a Protection Profile using the language of the Common Criteria by choosing the appropriate security functionalities and level of assurance from the Common Criteria lists. Similarly, product vendors can specify the security functionalities which exist in their product as well as the tests performed to verify proper implementation in a "Security Target."

SECTION II - TCSEC STATUS AND MIGRATION TO THE COMMON CRITERIA

5. The NSA in-house Trusted Product Evaluation Program (TPEP), as well as NSA's Trust Technology Assessment Program (TTAP) which uses accredited private sector evaluation laboratories, are presently evaluating products based upon the TCSEC standard. Products currently being evaluated under these programs will continue. However, as of 1 February 1999, these programs will no longer accept new evaluations based upon the TCSEC. Any new products accepted by these programs after 1 February 1999 must be evaluated using Common Criteria specifications. By the end of the year 2001, all products which were formerly evaluated against the TCSEC will have either become obsolete or, if they have maintained their TCSEC rating and are still in use, will be transitioned to a Common Criteria evaluation rating. Accordingly, agencies should be aware that as of 31 December 2001, all TCSEC ratings will be considered invalid.

6. NSA has already translated the TCSEC "C2" and "B1" classes for operating systems into Common Criteria-based specifications (or "Protection Profiles"). Thus, U.S. Government departments and agencies which have been relying on C2 or B1 evaluations for acquisition purposes will still be able to procure "C2" or "B1" compliant products. However, these products will have been evaluated to Common Criteria-based versus TCSEC-based specifications. These specifications are available on the Internet at URL: http:// www.radium.ncsc.mil/tpep/library/protection_profiles/index.html. NSA is in the process of translating the TSCEC "B2" and "B3" classes into Common Criteria-based Protection Profiles. There are no plans to translate the TCSEC "A1" class into a Common Criteria-based Protection Profile.

7. The use of the Trusted Network Interpretation (TNI) of the TCSEC has been limited in scope and not widely applicable to current networking technology. Therefore, there are no plans to draft Common Criteria Protection Profiles that correspond to the TNI classes. Rather, NSA and our partners in an initiative known as the Information Assurance Framework activity are presently drafting Protection Profiles for a wide range of technologies which can be used as part of solution sets. Currently, Protection Profiles for Firewalls have been completed and may be viewed at the URL previously mentioned.

8. The National Computer Security Center (NCSC) Rainbow Series comprises a library of guidance documents to aid in the evaluation and use of trusted products. The entire series of these documents are being reviewed and each document within the series is being categorized as to its usefulness under the Common Criteria. A list of these documents and their applicability to the Common Criteria will be published by June 1999, and will specify those documents that are no longer applicable as well as those documents which will be revised to reference Common Criteria-based requirements.

SECTION III - SUMMARY

9. All U.S. Government department and agencies should plan for the migration from use of the TCSEC to the Common Criteria. It is encouraged and recommended all personnel involved in the Information Assurance field become familiar with the Common Criteria and participate in the Information Assurance Framework activities. Overview courses on the Common Criteria are available through NSA or through the NIAP.

10. Further information on the following activities can be obtained through the following Internet URLs:

NIAP:	http://niap.nist.gov
Common Criteria:	http://csrc.nist.gov/cc/
TCSEC/TPEP/TTAP:	http://www.radium.ncsc.mil/tpep/index.html
IA Framework:	http://www.nsff.org

11. Questions pertaining to this Advisory Memorandum should be directed to the National Information Support Center 1-800-688-6115.