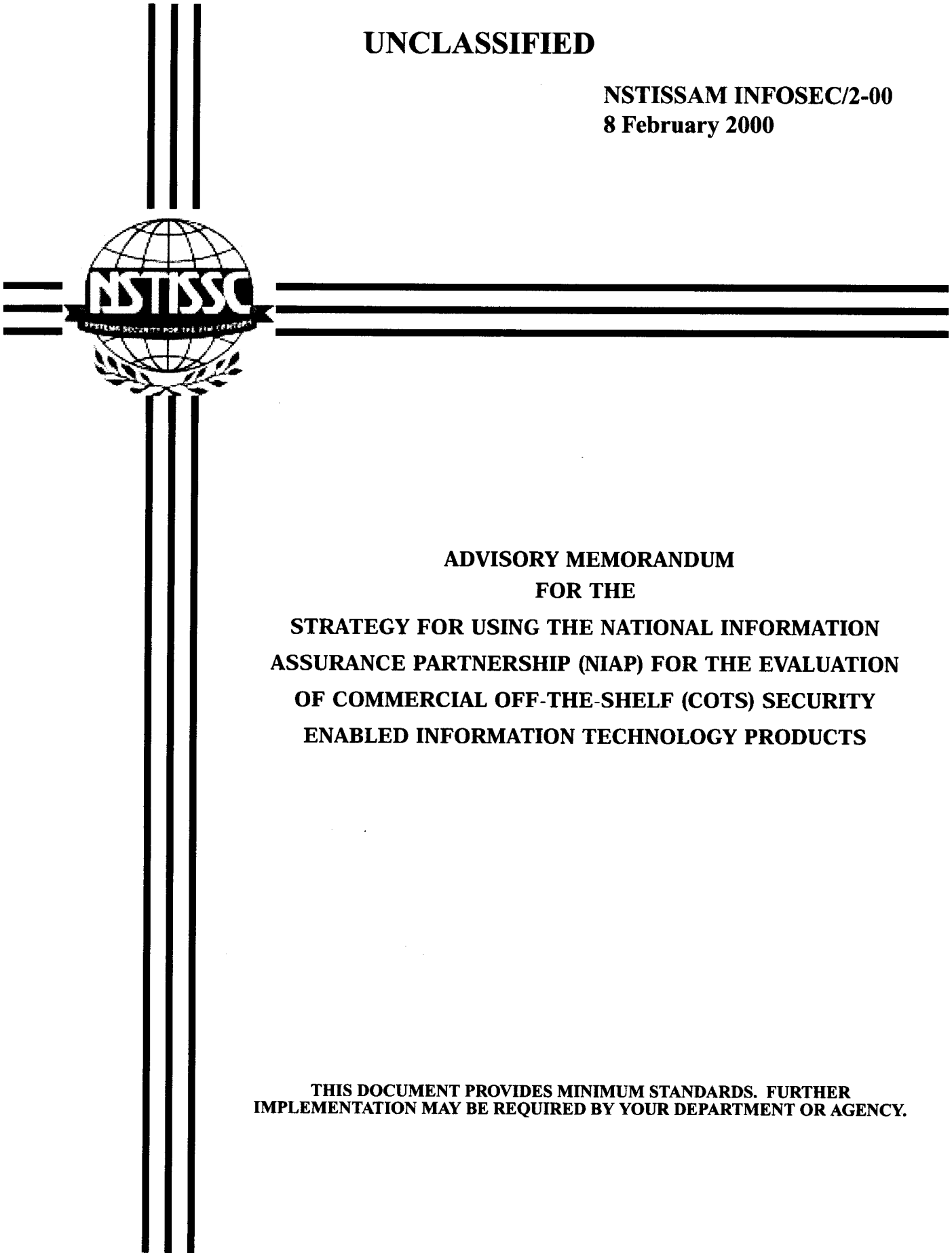
UNCLASSIFIED

NSTISSAM INFOSEC/2-00
8 February 2000



ADVISORY MEMORANDUM FOR THE STRATEGY FOR USING THE NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP) FOR THE EVALUATION OF COMMERCIAL OFF-THE-SHELF (COTS) SECURITY ENABLED INFORMATION TECHNOLOGY PRODUCTS

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

UNCLASSIFIED

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 strategy behind the National Information Assurance Partnership (NIAP) for the evaluation of commercial off-the-shelf (COTS) security enabled information technology products and, from a practical standpoint, details its implementation. It also serves to document the respective roles of the National Security Agency (NSA), the National Institute of Standards and Technology (NIST) and the accredited laboratories in the overall COTS evaluation and validation process.

2. Issuance of the document represents another step in a continuing effort to keep departments and agencies apprised of significant information systems security or information assurance developments which may impact on the operations and activities of their respective organizations. This advisory supplements information previously published on the evaluation of COTS products which was published in NSTISSAM COMPUSEC/1-99, Subject: Advisory Memorandum on the Transition From the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation, dated 11 March 1999.

MICHAEL V. HAYDEN
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 STRATEGY FOR USING THE NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP) FOR THE EVALUATION OF COMMERCIAL OFF-THE-SHELF (COTS) SECURITY ENABLED INFORMATION TECHNOLOGY PRODUCTS

SECTION I - REFERENCES

a. NSTISSAM COMPUSEC/1-99, Advisory Memorandum on the Transition from the Trusted Computer System Evaluation Criteria (TCSEC) to the International Common Criteria for Information Technology Security Evaluation, dated 11 March 1999

b. NSTISSAM COMPUSEC/1-98, The Role of Firewalls and Guards in Enclave Boundary Protection, dated December 1998

SECTION II - GENERAL BACKGROUND

1. Reference a. provided guidance to U.S. Government departments and agencies on the transition from the Trusted Computer System Evaluation Criteria (better known as the Orange Book) to the International Common Criteria as the basis for evaluation of commercial off-the-shelf (COTS) security and security-enabled information technology (IT) products. It further advised that the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) had established the National Information Assurance Partnership (NIAP) to accredit private sector laboratories to evaluate products and systems in accordance with the Common Criteria.

2. This advisory provides additional information on the NIAP process for evaluating COTS security and security-enabled IT products, the NIAP product certificate, and the NIAP Validated Products List (VPL). Additionally, this advisory provides guidance on the NSA strategy to use the Common Criteria and the NIAP to certify security and security-enabled IT products for the national security community.

SECTION III - THE NATIONAL INFORMATION ASSURANCE PARTNERSHIP

3. The NIAP is a collaborative effort between NIST and NSA designed to meet the security evaluation needs of both IT producers and users. The program fosters the availability of standardized specifications and test methods for evaluating the security robustness of COTS security and security-enabled IT products. In addition, it is designed to foster the development of commercial testing laboratories to provide security evaluation services which will meet the demands of both producers and users. NIAP testing will replace the COTS IT product evaluations previously performed by NSA under the Trusted Product Evaluation Program (TPEP) and other programs.

4. The NIAP program requires an extensive accreditation process for all commercial laboratories. This process, performed by the National Voluntary Laboratory Accreditation Program (NVLAP), an internationally recognized accreditation body, analyzes the laboratory quality processes against the International Standards Organization (ISO) Guide 25 and ISO

9000 quality principles. Additionally, the laboratories are analyzed and tested on their ability to interpret and apply the Common Criteria (CC) and its associated Common Evaluation Methodology. Once accredited by NVLAP and accepted by NIAP into the program, a laboratory will contract directly with a sponsor (usually a product manufacturer) to have a security or security-enabled IT product evaluated. NIAP assigns a government validator to each product evaluation to monitor the laboratory compliance with the CC as well as the quality and consistency of work being performed.

5. The laboratory will evaluate the product against a Security Target (ST) provided by the vendor. The ST is a CC-based document which describes the product's security functionality claims, as well as the desired level of evaluation (specified as an Evaluated Assurance Level (EAL)) that the laboratory performs to verify whether the product meets its security claims. If the product meets the ST criteria, the laboratory issues a report to NIAP documenting the results of the analysis performed by the laboratory. NIAP reviews the laboratory report to determine if the analysis was consistent with CC requirements. If consistent, NIAP will issue a certificate to the sponsor of the evaluation validating that the product is consistent with the claims in the ST. This certificate is signed by the NIST and NSA senior level executives responsible for the NIAP program and the product is listed on the NIAP VPL which can be found at:

http://niap.nist.gov/cc-scheme/ValidatedProducts.html

6. **Important:** Products listed on the NIAP VPL should not be interpreted as an NSA or a NIST endorsement or certification of the product for government use. It is only a validation that the product met its security claims consistent with the level of analysis performed by the laboratory and that the laboratory analysis performed was consistent with CC and Common Evaluation Methodology requirements. For example, a product may claim that it performs access control using a password entry system with a two character password. If the laboratory finds that indeed the product provides access control using a two character password, the product has successfully met its claim and would be awarded a certificate signed by NIST and NSA. However, this does not mean that either NIST or NSA endorse a product employing a two character password as appropriate for government access control requirements.

7. **Important**: Security vulnerabilities may exist in a product for which a validation certificate was issued by NIAP if such vulnerabilities would have been only discovered as a result of a level of evaluation (i.e., EAL) higher than that specified in the security target. Government integrators are advised to carefully read the ST and NIAP validation report to determine if the product security functionality and evaluation level performed is appropriate for a specific application.

SECTION IV - USE OF NIAP FOR THE EVALUATION OF COTS SECURITY AND SECURITY-ENABLED IT PRODUCTS

8. The migration from NSA evaluation of COTS products to the NIAP evaluation program is based upon several factors. Over the past decade, there has been a tremendous growth in the availability of COTS security and security-enabled IT products, and a corresponding increasing demand for these products to be evaluated. This increased availability of products, coupled with rapid product updates and new releases, has led to a dramatic increase in the time required to service evaluation requests. When completed, the evaluation was often outdated as the evaluated version of the product was no longer supported by the manufacturer. A move to commercial evaluation facilities will allow evaluations to be

performed at a faster rate than previous NSA evaluations as commercial laboratories are able to react more quickly to market demands.

9. In order to achieve fairness in the market place and to avoid government competition with the NIAP commercial laboratory evaluation program, NSA will no longer service customer requests for the evaluation of COTS security or security-enabled IT products. Government customers should look to the NIAP program for their security and security-enabled COTS IT product evaluation requirements. NSA will continue to evaluate U.S. Government-developed security products, as well as augment COTS evaluations higher than EAL4 provided they have first undergone a preliminary NIAP evaluation.

SECTION V - GUIDANCE REGARDING THE USE OF SECURITY AND SECURITY-ENABLED COTS IT PRODUCTS

10. To provide customer guidance on recommended minimum essential security robustness requirements for security and security-enabled COTS IT products, NSA will issue a series of technology-based Common Criteria (CC) Protection Profiles. These Protection Profiles are being developed under the auspices of the Information Assurance Technology Framework (IATF) in cooperation with the user community and security vendors. More detailed information on the IATF is available at:

http://www.iatf.net

Recommended protection profiles for firewalls were previously addressed in reference b., and are available at:

http://www.radium.ncsc.mil/tpep/

Protection Profiles are also being developed for levels of robustness designated as:

a. Basic
b. Medium
c. High

11. Protection profiles will take into account the sensitivity of the data, the level of threat, the state of the art of COTS security products, and the cost and time for an evaluation to be completed.

Important: It must be emphasized that security products which meet these profiles may still contain vulnerabilities. Nevertheless, the profiles will be the best that can be accomplished at the present time based upon the rate of change and the maturity of COTS security product development processes. In designing Protection Profiles for differing levels of robustness, the threat to the information is addressed based upon the value of the information as well as the environment in which the product will be placed. For example, the level of value of classified information is defined to be higher than that for unclassified data. Similarly, the scope of evaluation specified in the protection profiles is based upon the threat perceived to the data in that environment. Additionally, the scope of evaluation must also take into account the economic costs in performing that evaluation in terms of dollars and time and the existing state of the art of COTS security and security enabled technology. For example, while it may be desirable to perform a full source code analysis on all firewalls destined for an unclassified but sensitive-mission support data environment, the economic costs of such an analysis when weighed against the value of this information makes this approach untenable. Firewall vendors

are not willing to pay the attendant costs for this type of evaluation, and it is unlikely that any such evaluation could be accomplished before a new version of the firewall would be released.

SECTION VI - NSA CERTIFICATIONS

12. NSA will certify Protection Profiles determined to be compliant with the IATF. Protection Profiles so certified will be identified on the NSA home page at:

http://www.radium.ncsc.mil/tpep

Additionally, where a protection profile does not exist, government customers may request NSA to review and certify vendor security targets (STs) to determine if the product's proposed security functionality and level of evaluation are appropriate for the application where the customer intends to use the product. Products then evaluated and validated by NIAP approved laboratories against NSA-certified Protection Profiles or STs will also be noted on NSA's web page.