

DoD 5200.28-STD
Supersedes
CSC-STD-001-83, dtd 15 Aug 83
Library No. S225,711

DEPARTMENT OF DEFENSE STANDARD

DEPARTMENT OF
DEFENSE
TRUSTED COMPUTER
SYSTEM EVALUATION
CRITERIA

DECEMBER 1985

December 26, 1985

FOREWORD

This publication, DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," is issued under the authority of an in accordance with DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," and in furtherance of responsibilities assigned by DoD Directive 5215.1, "Computer Security Evaluation Center." Its purpose is to provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies in support of the overall ADP system security policy, evaluation and approval/accreditation responsibilities promulgated by DoD Directive 5200.28.

The provisions of this document apply to the Office of the Secretary of Defense (ASD), the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, the Defense Agencies and activities administratively supported by OSD (hereafter called "DoD Components").

This publication is effective immediately and is mandatory for use by all DoD Components in carrying out ADP system technical security evaluation activities applicable to the processing and storage of classified and other sensitive DoD information and applications as set forth herein.

Recommendations for revisions to this publication are encouraged and will be reviewed biannually by the National Computer Security Center through a formal review process. Address all proposals for revision through appropriate channels to: National Computer Security Center, Attention: Chief, Computer Security Standards.

DoD Components may obtain copies of this publication through their own publications channels. Other federal agencies and the public may obtain copies from: Office of Standards and Products, National Computer Security Center, Fort Meade, MD 20755-6000, Attention: Chief, Computer Security Standards.

Donald C. Latham
Assistant Secretary of Defense
(Command, Control, Communications, and Intelligence)

ACKNOWLEDGEMENTS

Special recognition is extended to Sheila L. Brand, National Computer Security Center (NCSC), who integrated theory, policy, and practice into and directed the production of this document.

Acknowledgment is also given for the contributions of: Grace Hammonds and Peter S. Tasker, the MITRE Corp., Daniel J. Edwards, NCSC, Roger R. Schell, former Deputy Director of NCSC, Marvin Schaefer, NCSC, and Theodore M. P. Lee, Sperry Corp., who as original architects formulated and articulated the technical issues and solutions presented in this document; Jeff Makey, formerly NCSC, Warren F. Shadle, NCSC, and Carole S. Jordan, NCSC, who assisted in the preparation of this document; James P. Anderson, James P. Anderson & Co., Steven B. Lipner, Digital Equipment Corp., Clark Weissman, System Development Corp., LTC Lawrence A. Noble, formerly U.S. Air Force, Stephen T. Walker, formerly DoD, Eugene V. Epperly, DoD, and James E. Studer, formerly Dept. of the Army, who gave generously of their time and expertise in the review and critique of this document; and finally, thanks are given to the computer industry and others interested in trusted computing for their enthusiastic advice and assistance throughout this effort.

CONTENTS

FOREWORD. i
ACKNOWLEDGMENTS ii
PREFACE v
INTRODUCTION. 1

PART I: THE CRITERIA

1.0 DIVISION D: MINIMAL PROTECTION. 9
2.0 DIVISION C: DISCRETIONARY PROTECTION. 11
 2.1 Class (C1): Discretionary Security Protection . . 12
 2.2 Class (C2): Controlled Access Protection. 15
3.0 DIVISION B: MANDATORY PROTECTION. 19
 3.1 Class (B1): Labeled Security Protection 20
 3.2 Class (B2): Structured Protection 26
 3.3 Class (B3): Security Domains. 33
4.0 DIVISION A: VERIFIED PROTECTION 41
 4.1 Class (A1): Verified Design 42
 4.2 Beyond Class (A1). 51

PART II: RATIONALE AND GUIDELINES

5.0 CONTROL OBJECTIVES FOR TRUSTED COMPUTER SYSTEMS. 55
 5.1 A Need for Consensus 56
 5.2 Definition and Usefulness. 56
 5.3 Criteria Control Objective 56
6.0 RATIONALE BEHIND THE EVALUATION CLASSES. 63
 6.1 The Reference Monitor Concept. 64
 6.2 A Formal Security Policy Model 64
 6.3 The Trusted Computing Base 65
 6.4 Assurance. 65
 6.5 The Classes. 66
7.0 THE RELATIONSHIP BETWEEN POLICY AND THE CRITERIA 69
 7.1 Established Federal Policies 70
 7.2 DoD Policies 70
 7.3 Criteria Control Objective For Security Policy . . 71
 7.4 Criteria Control Objective for Accountability. . . 74
 7.5 Criteria Control Objective for Assurance 76
8.0 A GUIDELINE ON COVERT CHANNELS 79

9.0 A GUIDELINE ON CONFIGURING MANDATORY ACCESS CONTROL
FEATURES 81

10.0 A GUIDELINE ON SECURITY TESTING 83

 10.1 Testing for Division C 84

 10.2 Testing for Division B 84

 10.3 Testing for Division A 85

APPENDIX A: Commercial Product Evaluation Process. 87

APPENDIX B: Summary of Evaluation Criteria Divisions 89

APPENDIX C: Summary of Evaluation Criteria Classes. 91

APPENDIX D: Requirement Directory. 93

GLOSSARY. 109

REFERENCES. 115

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.