NCE & TECHNOLOGY:

AUDIT AND EVALUATION OF COMPUTER SECURITY

NBS Special Publication 500-19
U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards[1] was established by an act of Congress 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 consists of the Institute for Basic Standards, the Institute for Materials Research, the Institute for Applied Technology, the Institute for Computer Sciences and Technology, the Office for Information Programs, and the Office of Experimental Technology Incentives Program.

THE INSTITUTE FOR BASIC STANDARDS provides the central basis within the United States of a complete and consistent system of physical measurement; coordinates that system with measurement systems of other nations; and furnishes essential services leading to accurate and uniform physical measurements throughout the Nation's scientific community, industry, and commerce. The Institute consists of the Office of Measurement Services, and the following center and divisions:

Applied Mathematics — Electricity — Mechanics — Heat — Optical Physics — Center for Radiation Research — Laboratory Astrophysics[2] — Cryogenics[2] — Electromagnetics[2] — Time and Frequency[2].

THE INSTITUTE FOR MATERIALS RESEARCH conducts materials research leading to improved methods of measurement, standards, and data on the properties of well-characterized materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; and develops, produces, and distributes standard reference materials. The Institute consists of the Office of Standard Reference Materials, the Office of Air and Water Measurement, and the following divisions:

Analytical Chemistry — Polymers — Metallurgy — Inorganic Materials — Reactor Radiation — Physical Chemistry.

THE INSTITUTE FOR APPLIED TECHNOLOGY provides technical services developing and promoting the use of available technology; cooperates with public and private organizations in developing technological standards, codes, and test methods; and provides technical advice services, and information to Government agencies and the public. The Institute consists of the following divisions and centers:

Standards Application and Analysis — Electronic Technology — Center for Consumer Product Technology: Product Systems Analysis; Product Engineering — Center for Building Technology: Structures, Materials, and Safety; Building Environment; Technical Evaluation and Application — Center for Fire Research: Fire Science; Fire Safety Engineering.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides technical services designed to aid Government agencies in improving cost effectiveness in the conduct of their programs through the selection, acquisition, and effective utilization of automatic data processing equipment; and serves as the principal focus wthin the executive branch for the development of Federal standards for automatic data processing equipment, techniques, and computer languages. The Institute consist of the following divisions:

Computer Services — Systems and Software — Computer Systems Engineering — Information Technology.

THE OFFICE OF EXPERIMENTAL TECHNOLOGY INCENTIVES PROGRAM seeks to affect public policy and process to facilitate technological change in the private sector by examining and experimenting with Government policies and practices in order to identify and remove Government-related barriers and to correct inherent market imperfections that impede the innovation process.

THE OFFICE FOR INFORMATION PROGRAMS promotes optimum dissemination and accessibility of scientific information generated within NBS; promotes the development of the National Standard Reference Data System and a system of information analysis centers dealing with the broader aspects of the National Measurement System; provides appropriate services to ensure that the NBS staff has optimum accessibility to the scientific information of the world. The Office consists of the following organizational units:

Office of Standard Reference Data — Office of Information Activities — Office of Technical Publications — Library — Office of International Standards — Office of International Relations.

---

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington, D.C. 20234.

[2] Located at Boulder, Colorado 80302.

COMPUTER SCIENCE & TECHNOLOGY:

Audit and Evaluation of Computer Security

Proceedings of the NBS Invitational Workshop
held at Miami Beach, Florida, March 22-24, 1977

Edited by:

Zella G. Ruthberg

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D. C. 20234

Robert G. McKenzie

General Accounting Office
Washington, D. C. 20548

Session Chairpersons;

William E. Perry
C. O. Smith
Blake Greenlee
Carl Hammer
W. H. Murray
Clark Weissman
Leonard I. Krauss
Jerry FitzGerald
Richard D. Webb
Hart J. Will

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, Secretary
Dr. Sidney Harman, Under Secretary
Jordan J. Baruch, Assistant Secretary for Science and Technology
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Acting Director

Issued October 1977

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.

National Bureau of Standards Special Publication 500-19

Nat. Bur. Stand. (U.S.), Spec. Publ. 500-19, 256 pages (Oct. 1977)
CODEN: XNBSAV

Library of Congress Catalog Card Number: 77-600045

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1977

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402
Price $4—Stock No. 003-003-01848-1

FOREWORD

The increasing use of computers by Government and private organizations for the storage and manipulation of records of all kinds--personal as well as of a business nature--has placed computers and the systems in which they reside in an extremely sensitive position in our society. The needs of the individual as well as Government and private organizations require that this data and their resident systems be accurate and reliable. These needs also require that this data and these systems be given adequate protection from threats and hazards. The establishment of secure computer systems is the way in which the computer community assures the users of such systems that all of these requirements are being met.

The auditing and evaluating of computer systems for adequate security has been a natural outgrowth of this widening interest in this area. Controls that provide computer security are of interest to both the financial and internal auditors and has been made a subject of special consideration by organizations such as the Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the EDP Auditors Associtation.

The National Bureau of Standards, with the support of the U.S. General Accounting Office, sponsored an invitational workshop in March of 1977 to explore the subject of "Audit and Evaluation of Computer Security." Leading experts in the audit and computer communities were invited to share their thoughts and develop a consensus view on ten aspects of the subject. These Proceedings are the results of that meeting.

To all those concerned with the audit and evaluation of computer security today, we at the National Bureau of Standards offer this series of consensus reports for your consideration. The views expressed do not necessarily reflect those of the National Bureau of Standards, the U. S. General Accounting Office, or any of the organizations that sponsored an individual at the workshop. However, these reports do reflect the composite thoughts of a group that deserves your serious attention.

M. Zane Thornton
Acting Director
Institute for Computer
Sciences and Technology

PREFACE

The National Bureau of Standards (NBS) initiated a Task Group within the Federal Information Processing Standards (FIPS) program in 1973 to develop standards in Computer Systems Security. Task Group 15 (TG-15) was composed of representatives from private industry as well as Federal, State and local governments. The NBS Invitational Workshop on Audit and Evaluation of Computer Security was organized as one phase of a two-phase project defined by the Task Group in this important area of computer security. These Proceedings are the result of phase one. The second phase will be to adapt this information to the needs of Federal agencies in the form of Federal Information Processing Guidelines. This latter effort will be carried out by a working group convened for this purpose and will result in a FIPS publication by NBS.

The General Chairman and organizer of the Workshop was Robert G. McKenzie of the U.S. General Accounting Office. As leader of the TG-15 project on computer security auditing, he initiated and planned the Workshop and co-edited these Proceedings. Mr. McKenzie is an audit manager at GAO and has conducted a number of reviews of computer security of proposed and on-going systems in the Federal Government.

The General Vice-Chairman of the Workshop was Zella G. Ruthberg of the National Bureau of Standards. As NBS coordinator of the TG-15 security audit project, Mrs. Ruthberg worked closely with Mr. McKenzie on the planning, acted as the Workshop arrangements chairman, and is co-editor of these Proceedings. She has conducted a wide range of projects in computer science at NBS and most recently has become active in the managerial procedures required for computer security.

Mr. S. Jeffery, Chief of the Systems and Software Division of the Institute for Computer Sciences and Technology of NBS, headed the NBS staff at the Workshop. Mr. Jeffery has been active in the formulation of policy concerning the effective utilization of computers within the Federal Government and is manager of the computer program at NBS. This program provided the needed technical and administrative support for this Workshop.

I would like to thank all of the particitpants in this Workshop, the Chairmen and Recorders of the sessions, and the three individuals named above for the success of the Workshop. The products to be derived from the Workshop and subsequent efforts in this area will have far-reaching, beneficial effects on the use of computers throughout the country.

Dennis K. Branstad
Chairman, TG-15

ABSTRACT

The National Bureau of Standards, with the support of the U.S. General Accounting Office, sponsored an invitational workshop on "Audit and Evaluation of Computer Security," held in Miami Beach, Florida on March 22-24, 1977. Its purpose was to explore the state-of-the-art in this area and define appropriate subjects for future research. Leading experts in the audit and computer communities were invited to discuss the subject in one of ten sessions, each of which considered a different aspect. A consensus report was produced by each of the ten sessions and these reports form the body of these Proceedings. The ten topics reported on are: Internal Audit Standards, Qualifications and Training, Security Administration, Audit Considerations in Various System Environments, Administrative and Physical Controls, Program Integrity, Data Integrity, Communications, Post-Processing Audit Tools and Techniques, and Interactive Audit Tools and Techniques.

KEYWORDS: Audit standards, audit techniques, audit tools, audit training, communications security, computer controls, computer security, data integrity, interactive audit, internal audit, post-processing audit, program integrity.

ACKNOWLEDGEMENTS

The success of the Workshop was dependent on the work of many people. We would particularly like to take this opportunity to thank all the Session Chairmen, the Session Recorders, and the attendees for their efforts in behalf of this Workshop. We would also like to thank the session coordinators Robert V. Jacobson, John Panagacos, and Thomas C. Lowe for making things run smoothly while the Workshop was taking place; and Dennis K. Branstad for photographing scenes from the Workshop.

THE EDITORS

TABLE OF CONTENTS