UCID - 16738

This is an informal report intended primarily for internal or limited external distribution. The opinions and conclusions stated are those of the author and may or may not be those of the laboratory.

MASTER

LAWRENCE LIVERMORE LABORATORY

University of California/Livermore, California

OBTAINING COMPUTER DATA PRIVACY
THROUGH ACCREDITATION OF COMPUTER CENTERS

Douglas A. Webb, Ph.D.

Robert P. Abbott

March 1975

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Energy Research and Development Administration, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

Prepared for U.S. Atomic Energy Commission under contract no. W-7405-Eng-48

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

OBTAINING COMPUTER DATA PRIVACY
THROUGH ACCREDITATION OF COMPUTER CENTERS

Douglas A. Webb, Ph.D.
Robert P. Abbott

RISOS PROJECT
LAWRENCE LIVERMORE LABORATORY
LIVERMORE, CALIFORNIA 94550

March 1974

THE RISOS PROJECT IS SPONSORED BY THE ADVANCED RESEARCH PROJECTS
AGENCY OF THE DEPARTMENT OF DEFENSE UNDER ARPA ORDER NO. 2166

OBTAINING COMPUTER DATA PRIVACY THROUGH ACCREDITATION OF COMPUTER CENTERS

INTRODUCTION

Because of the new Privacy Act and the Freedom of Information Act, we expect greater emphasis will be given to insure data privacy in data processing installations.

How is data privacy measured?

Who says that an installation's data is protected?

How can a Data Processing manager measure his installation's capability for protecting data from misuse?

These are questions we should consider. One approach for answering these is through accreditation.

ACCREDITATION

Accreditation is a means of determining the level of data privacy as measured against a stated practical norm (i.e., not a norm that says no one can misuse a data bank). It is not a method of establishing a yes/no-100% answer to the question of an installation's software insuring data privacy.

ACCREDITATION COMMISSION

We recommend that an Accreditation Commission, similar to the Joint Commission on Hospital Accreditation, be formed to perform the following functions:

- Establish the general principles, objectives, or goals of software security as they relate to data privacy.
- Set standards that support and define the principles
- Develop interpretations or guidelines that explain and give practical examples for applying the principles and standards.
- Establish a formal methodology of accrediting data processing installations for purposes of privacy.
- Perform accreditation surveys and report results on an on-going basis.

SUGGESTED IMPLEMENTATION OF THE ACCREDITATION PROCESS

The principles, standards and interpretations can be modified periodically as times and needs change. The Commission would solicit opinions and recommendations from various government agencies, Data Processing societies and consumer advocate groups.

The Accreditation Commission can assign capable people (or go themselves) to visit a Data Processing installation and make an evaluation of the site's software security measures in terms of the data privacy provided.

The evaluation or survey is made relative to an established norm. This norm is defined in terms of general principles, supporting standards and specific interpretations.

The process may be set up similar to the way in which CPA firms give opinions on the accuracy and fairness of the financial reports of companies. The CPA report or opinion is a statement made by a recognized, capable and competent firm attesting that they have: 1) examined or audited (a set of listed) items; 2) made the examination in accordance with generally accepted auditing standards, and included necessary tests of the items and 3) reported any items that do not conform with generally accepted accounting principles.

The Data Processing installation can (in part) set the level of accreditation as they see and define the need for data privacy. Some aspects will be set by others - the Commission, Congress, individuals.

The period of accreditation could vary from daily examinations to one every two to five years. This will depend in part on the installation--similar to setting the level of accreditation.

SUPPORTIVE REASONS FOR THIS APPROACH

There is an established need with the new Privacy Act and the Freedom of Information Act to implement some form of accreditation function.

There is a historical precedent for a Commission - type of accreditation. Specifically, mandatory accreditation was imposed on hospitals by the Medicare Law.

The approach is flexible, it could be voluntary to some, mandatory to others. It does not have the stigma or real problems of legal requirements (e.g. it can be modified without a lot of red tape).

The standards apply to all Data Processing installations, but both the methods of meeting the standards and the accepted level of meeting the standards will vary.

Data Processing installations will find the approach provides a useful index for evaluating its level of data privacy. A systematic evaluation by a peer group shows an installation has: 1) collaborated to seek excellence, 2) accepted outside appraisal and 3) demonstrated conformance with professionally developed and nationally applied criteria.

This approach provides a workable means for strengthening the Privacy Act and assuring the public that a professional group is taking action to implement checks.

THINGS TO BE DONE

- Determine levels of accreditation
- Determine costs - 1) for each survey
 2) for implementing necessary recommendations
 3) for maintaining privacy
- Set principles - standards - interpretations
- Establish a formal methodology
- Prepare a statement of accreditation
- Determine who will make up the Commission and who will make surveys.

OPEN QUESTIONS

1. Level of standards and principles, i.e., how specific is each; how much leeway?
2. Classes of installations or levels of data processing. Are there different standards for each class or some basic standards for all and more stringent specs for more "important" facilities ("important" in terms of both data in the system and risk of compromise)?
3. Level of people to serve on Commission. Are they permanent or do they rotate?
4. Who should establish guidelines - e.g. NBS-ACM-"Call for recommendations".
5. Are intangible items considered, such as quality of people, number of programs and size of system?
6. Are the recommendations made by the Commission for improving data privacy mandatory or just suggestions?
7. What are the legal limits or responsibilities of carrying out recommendations?

GLOSSARY

1. Accreditation - The act of vouching that an installation meets prescribed standards of quality or a norm.
2. Attest - To affirm the truthfulness or validity of statements.
3. Audit - A formal examination and verification of accounts.
4. Certification - The act of attesting authoritatively that an installation meets a prescribed standard of quality; carries with it the notion of legality.
5. Freedom of Information Act - Public Law 93-502 - designed to make available to the public, indexes, identifying information and documents of government agencies.
6. Interpretation - An explanation or guideline to assist in understanding and applying standards.
7. Principle - A primary or basic doctrine, a fundamental objective.
8. Privacy Act - Public Law 93-579 - designed to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, and to establish a Privacy Protection Study Commission.
9. Standard - A rule or norm established by authority for measuring quality; a standard applies to a given principle.

DISTRIBUTION

R. Abbott	40	L-307
D. Webb	5	L-307
TID	5	L- 3
TIC	2	Oakridge

NOTICE

"This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Energy Research & Development Administration, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately-owned rights."