0. TABLE OF CONTENTS

1. Procedures

1.1 Purpose. This handbook provides the procedures for the development, implementation, and maintenance of the Bureau of Indian Affairs' (BIA) information resources security program. This handbook addresses security problems and provides more visibility to security concerns by combining all the requirements and responsibilities for information resources security into one handbook and requiring the establishment of one position to coordinate information resources security activities.

1.2 Scope. This handbook is concerned with non-national security information only.

1.3 Security Program Components. Successful implementation of an information resources security program depends upon accurately determining potential risks and instituting safeguards to minimize them. Every BIA information system and every information technology facility operated by or on behalf of the BIA shall be protected.

1.4 Risk Analysis.

A. Performance. A risk analysis is the first step in establishing a security program. Risk analyses shall be performed for all information technology facilities, all automated application systems, and all manual application systems covered by the Privacy Act. The extent of the risk analysis performed shall be commensurate with the magnitude and use of the resources to be protected. The risk analysis shall accomplish the following:

(1) Identify both the nature and potential source of all physical, personnel, administrative, and technical threats to a specific facility, installation, or system.

(2) Determine the probability of occurrence of each potential threat and the likely extent of damage.

(3) Evaluate the nature of the information being stored, processed, or communicated and determine whether it should be designated "sensitive".

(4) Determine both the financial and time cost

and the impact which would result from the loss or misuse of information resources.

(5) Propose safeguards based upon the above analysis.

B. Frequency of Occurrence.

(1) Information Technology Facilities and Automated Systems. A risk analysis shall be performed at least every five years if one has not been performed within that timeframe under the following special circumstances: when planning the development of a new system or facility, when significant changes are made to the nature or relative sensitive of data being processed or to the system or facility, and when environmental factors change in such a manner as to alter the threats presented. Those application systems covered by the Privacy Act shall also perform risk analyses under the conditions listed below for manual systems and also when the configuration (i.e., either hardware or software) of the computer on which the system is operated changes so as to create the potential for either greater or easier access.

(2) Manual Application Systems. A risk analysis shall be performed when a new system of records is proposed under the Privacy Act or when a change to an existing system is proposed which significantly alters the character of the system by increasing or changing the number or types of individuals on whom records are maintained; expanding the types or categories of information maintained; altering the purposes for which the information is used; or exempting records maintained on individuals from any provision of the Privacy Act.

1.5 Protection. Specific safeguards shall be employed to provide a reasonable means of counteracting each threat described in the risk analysis and for detecting actual or potential security violations. At a minimum, the following procedures shall be considered:

A. Physical Security. Appropriate practices and safeguards shall be utilized to minimize the following threats to those places where information and technological resources are located: theft, unauthorized or illegal access, accidental or intentional damage or destruction, improper use, and improper disclosure of information. The following general security standards apply:

(1) The computer facility shall not be easily accessible by the general public.

(2) Construction of each computer facility shall meet the requirements set forth by the National Fire Protection Association.

(3) Supporting equipment for each facility shall be protected.

(4) Each site shall be protected from natural hazards to the highest degree possible.

(5) Facilities shall be restricted to essential and authorized personnel.

(6) Each computer facility shall be subject to periodic inspection by fire prevention officials and shall be certified based upon the findings of the inspection.

(7) Fire drills shall be conducted periodically in order to test evacuation procedures.

(8) Safety personnel shall conduct courses which address fire emergencies throughout the BIA.

(9) U. S. Government (GSA/BIA) code requires that pipes, cables and wiring are wrapped in fire resistant materials. Precautionary measures to prevent the spreading of fire shall be included in all construction specifications throughout the BIA.

(10) A variety of fire prevention or retardant equipment shall be employed Bureauwide and consist of the following:

(a) A, B, and C rated fire extinguishing equipment.

(b) Water sprinkling systems.

(c) Automatic fire detection alarms, smoke alarms, and suppression systems.

(d) Fire Alarms.

B. Personnel Security. All Federal and contractor employees shall receive security clearances or certifications of computer access commensurate with the sensitivity of the information or computer facilities they manage or use. All employees using information and technological resources, subject to security measures in this handbook, shall be required to sign statements acknowledging their responsibility for the security of these resources. These statements shall be retained in the employee's official personnel folder.

C. Technical Security. Appropriate safeguards (such as password usage, encryption, security software) shall be utilized to prevent unauthorized access and use of information, data, and software resident on peripheral devices or storage media or in the process of being communicated via technological means. Password systems shall assure effective protection of the password database with the same protection rendered for private or sensitive information processed. Access to the BIA computer system shall be restricted to users who have an authorized user ID and password. In order to obtain a valid user ID and password, a Computer Access Request, BIA-3502 (Illustration 1) shall be completed. It shall be reviewed, approved, and signed by an authorized BIA Office/Program manager. The completed form shall be forwarded to:

Department of the Interior
Bureau of Indian Affairs
National Technical Support Center
BIA Security Officer
P.O. Box 888
Albuquerque, New Mexico 87103

(1) User passwords shall be assigned at the National Technical Support Center (NTSC) and two copies of the password shall be sent to the originator. One copy shall be maintained by the originator and one copy shall be acknowledged, signed, and returned to the NTSC.

(2) Once the signed acknowledgment has been received, it shall be placed in the security files. All user ID's and passwords shall be issued for the exclusive use of the persons to whom they are assigned.

(3) All passwords for former employees shall be removed immediately upon their separation from the BIA.

Passwords shall also be removed for those personnel no longer having a need to access BIA systems.

D. Administrative Security. Procedures shall be established and disseminated to ensure that all information resources are properly protected and that information technology resources are used only by authorized personnel.

1.6 Automated Application Safeguards. Specific procedures shall be followed to ensure that appropriate safeguards are incorporated into automated application systems. They include:

A. Determining appropriate security safeguards prior to system development or acquisition.

B. Conducting design reviews and system tests prior to system implementation to ensure that the system satisfies the approved security requirements.

C. Certifying, prior to implementation, that a new system satisfies applicable policies, regulations and standards and that its security safeguards are adequate.

D. Evaluating at least every three years the sufficiency of security safeguards for existing sensitive system.

1.7 Continuity of Operations Planning.

A. Information Technology Facilities and Automated Application Systems. A continuity of operations plan (COOP) shall be developed for each information technology facility and each automated application system to ensure that interruptions of service of whatever type or duration are kept to a minimum. The COOP shall be evaluated periodically to determine the continued appropriateness of the established procedures. It shall be revised when indicated by changes in software, equipment, or other related factors. At a minimum, the COOP shall address the following:

(1) Procedures for backup storage and recovery of data and software.

(2) Establishment of processing capabilities and procedures for transferring operations to an alternate site.

(3) Consistency between application system COOPs and the COOP of the information technology facility where the application is processed; and

(4) Annual testing of the COOP at large mainframe installations and other installations that provide essential BIA computer support.

B. Manual Application Systems. Continuity of operation plans shall be developed for all manual application systems containing vital records to ensure their continued protection and so that essential BIA activities can continue during periods of national emergency. These plans shall be reviewed annually and periodically tested under emergency conditions to ensure their adequacy.

1.8 Security Awareness Activities. BIA and contractor employees shall be adequately trained so that they may fulfill their security responsibilities. The level of security awareness activities in which employees participate are dependent upon their specific involvement with information resources. Information regarding employees' security awareness activities shall be retained in their official personnel folders. The following levels of security awareness participation will be utilized within the BIA:

A. "Orientation" which includes documents, briefings, and/or films designed to acquaint employees with the nature of risks associated with information resources and the use of security measures to counteract them. All new personnel shall be provided with security awareness training within 60 days of their appointment.

B. "Education" which includes classes and seminars designed to provide managers, owners, users, and custodians of information and information technology resources with a general understanding of how to implement security measures and how to determine if security breaches have occurred.

C. "Training" which includes more in-depth classes designed to provide owners and users, especially information technology professionals, with the ability to perform risk analyses, design protection programs, and evaluate the effectiveness of existing security programs.

1.9 Acquisition Planning. It is essential that appropriate safeguards be determined before the acquisition of information technology resources, not only to ensure the wise expenditure of funds, but also so that resources may be protected from the time of installation or implementation. To accomplish this, all contract specifications for the acquisition of hardware, software, software development, equipment maintenance, facility management, and related services must contain requirements for safeguards that encompass technical, administrative, personnel, and physical security.

1.10 Other Applicable Regulations. Personnel responsible for information resources security shall be knowledgeable of, and conform to, the regulations listed below to ensure proper adherence to security program components.

376	DM	Automated Data Processing
377	DM	Telecommunications
381	DM	Origination of Records and Information
382	DM	Records Operations
383	DM	Policies and Procedures for Implementing the Privacy Act of 1974
384	DM	Records Disposition
385	DM	Office Automation Technology
436	DM	Vital Records
441	DM	Clearances and Suitability Investigation Requirements
442	DM	National Security Information
443	DM	Industrial Security Program
444	DM	Physical Security

1.11 Review and Evaluation.

A. The Office of Data Systems shall conduct periodic reviews and evaluations of BIA information resources security programs to ensure compliance with Federal, Departmental, and BIA directives.

B. Each Central Office, Area, and Agency shall conduct annual reviews and evaluations of its information resources security program to determine its effectiveness and to recertify the adequacy of the installed security safeguards. These reviews may utilize existing reports, such as those for risk analyses, application system certifications, Privacy Act inspections, records management evaluations, the Departmental Control Evaluation Program, and Inspector General audits.

C. The output of these reviews shall serve as the basis for the annual BIA security plan and the assurance statement regarding the adequacy of BIA automated information system security that shall be submitted annually in accordance with OMB Circular No. A-123.

D. Copies of the reviews shall be provided upon completion to the Office of Inspector General and, upon request, to the Departmental Information Resources Security Administrator.

1.12 Reporting Requirements.

A. Security Plan. The Bureau Information Resources Security Administrator (refer to 35 BIAM 6.4D) shall annually develop a planning document (Report Control Number DOI-84-087) which describes BIA information resources security activities. This document shall be submitted for review to the Departmental Information Resources Security Administrator by December 15 of each year and shall, as a minimum, include the following:

(1) An overview of BIA information resources activities as they pertain to security issues, problems and solutions.

(2) A description of the current year accomplishments in implementing the BIA's information resources security program.

(3) An itemization of those activities which must be accomplished to implement an effective information resources security program in the BIA.

(4) A milestone schedule of information resources security activities planned for the upcoming year to include such activities as risk analyses to be performed, new or modified security procedures to be implemented, evaluations of existing security procedures, and security awareness activities.

B. Security Incidents. All security incidents shall be reported to the appropriate authorities. The type of incident encountered shall determine to whom it shall be reported. It is the responsibility of every employee to report all suspected, actual, or threatened incidents involving information resources to the authorities indicated below.

(1) Incidents involving physical, personnel and national security complaints and violations shall be reported to

the BIA Security Officer. This includes the destruction, physical abuse, or loss of technological resources.

(2) Incidents involving records and their unlawful removal, defacing, alteration, or destruction shall be reported to the Records Management Officer for subsequent notification of the BIA head and the National Archives and Records Administration.

(3) Incidents involving Privacy Act violations shall be reported to the BIA Privacy Act Officer for coordination of corrective action with the pertinent program/system manager.

(4) Incidents involving technological resources resulting in the loss of technology, fraud, or compromise/ disclosure of sensitive material shall be reported at the time of discovery to the BIRSA, the Departmental Information Resources Security Administrator, and the Office of Inspector General (OIG). This verbal report shall be followed with a written report containing a description of the incident, the system and location involved, and the corrective action taken. All computer hacker incidents shall be reported to the OIG via the OIG hotline, but via conventional means to the BIA and department. Other types of technological security incidents shall be reported only to the BIRSA and to the Departmental Security Administrator.

BIA-3502 — 01 90

ADP
SECURITY OFFICE
- - - - - - - - - -
#: _____
Date: ___ /___ /___

United States Department of the Interior
Bureau of Indian Affairs
Office of Data Systems
Computer Access Request

NEW: [ ] ADD: [ ] DELETE: [ ] CHANGE: [ ]
CURRENT USER ID: _____

****

REQUESTOR

User Name: _____ SSN #: ___ ___ ___ - ___ ___ - ___ ___ ___ ___

Title: _____ Office/Area/Agency: _____

Address: _____

City/State: _____ ZIP: _____

Telephone: FTS: _____ Commercial ( ) _____

REQUEST FOR PRIMARY ADP USE: _____

AMDAHL COMPUTERS: [ ] CICS TRANS: _____, _____, _____
_____, _____, _____

UNISYS:.....
B-1900: [ ] OTHER: [ ] _____
A-10: [ ] Request Date: ___ /___ /___

AUTHORIZED BY: _____ TITLE: _____
(Signature)

ISSUER

Computer Facility: _____
(Name and Location)

System Access: _____ Program/Appl: _____

Issued By: _____ Title: _____

Changed By: _____ Title: _____

Revoked By: _____ Title: _____

Account Number: _____ Date: ___ /___ /___

TO USER

**********WARNING**********

This User Id is issued for your EXCLUSIVE, INDIVIDUAL access to the computer. DO NOT SHARE IT WITH ANYONE OR USE IT FOR NONE OTHER THAN OFFICIAL BUSINESS. Unauthorized use of Government computer facilities is a CRIMINAL OFFENSE AND VIOLATIONS ARE PROSECUTABLE UNDER FEDERAL LAW.

USER ID: _____ PASSWORD: _____

I ACKNOWLEDGE RECEIPT AND ACCEPT THE RESPONSIBILITIES FOR THE USE OF THIS I.D.:

(Signature) _____

Sign and return this form to the ISSUER. You may make a copy, but it must be kept in a SECURED PLACE.

**********WARNING**********