DESIGN AND IMPLEMENTATION OF A SECURITY INFORMATION SYSTEM

(A CASE STUDY OF THE NIGERIAN POLICE)

BY

NWACHUKWU NNAMDI V.

REG. NO: CST/2008/288

DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

FACULTY OF NATURAL SCIENCES CARITAS UNIVERSITY, AMORJI-NIKE EMENE, ENUGU STATE

FOR

IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF BACHELOR OF SCIENCE (B.Sc.) IN COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

AUGUST, 2012.

APPROVAL PAGE

This project work written by **NWACHUKWU NNAMDI V.** has been approved for the department of computer science and information technology, Caritas University Enugu state.

…… ……..

NWACHUKWU NNAMDI V. Date

(Student)

……. …….

Mr. Ikpeama Chigozie Date

(Project Supervisor)

……. ……..

Dr. A. S. ARINZE Date

(Head of Department)

…….. ……..

External Examiner Date

CERTIFICATION PAGE

This is to certify that this project work was fully carried out by **NWACHUKWU NNAMDI V.** of the Department of Computer Science and information technology, Caritas University Amorji-Nike, Enugu state.

…… ……..

NWACHUKWU NNAMDI V. Date

(Student)

……. ……..

Mr. Ikpeama Chigozie Date

(Project Supervisor)

DEDICATION

This work is dedicated to God Almighty who in His infinite mercy gave me the good health and strength to do this research work. And also to my lovely parents Hon.& Mrs. Gozie Nwachuwu and my siblings for their help and encouragement.

To all my relations and friends, I remain grateful for your support.

ACKNOWLEDGEMENT

You can never know how important the other man can contribute to your existence and success until you look for him to tell you how you look and find him not. For this, I wish to acknowledge and appreciate all who blew the smoke into fire in one way or the other.

First, I wish to acknowledge God Almighty who has given me the life and from whose intelligence I share mine.

My sincere and heartfelt gratitude also goes to the Head of Department, Dr. A.S. Nwaeze, for his counsel, guidance and fatherly gestures throughout the period of this project and my overall academic work.

Next is my supervisor, Mr. Ikpeama Chigozie, who devoted his time to supervise, correct and criticize this research work to make it a reality.

I am very grateful to the committed team of lecturers (Mr. Ejike, Mrs. Chizoba Ezeme, Mr. Solomon, and Mr. Joseph Igwe and Mr. Prado) who have been instrumental to the wealth of knowledge I have acquired in the department of Computer Science and Information Technology. Words cannot express my gratitude to you all; you will always be remembered dearly.

I am also obliged to say a big "thank you" to my siblings. I can never forget my dear friends you stood by me amidst all troubles.

Finally, to the authors of books and libraries consulted to see this project a success. They remain ever green in my memory.

Thanks a lot.

TABLE OF CONTENTS

CHAPTER ONE

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

The principal objective of this project is to help Security Information Systems (SIS) especially NIGERIAN POLICE which is my case study in the area they encounter problems in securing security data-processing and efficient information system. This will be the solution given to handle this problem by transforming the existing manual information system into an automated form and overcome the existing problems of insecurity and delay in data processing. I decided to use an automated database system to enhance information storage and keep track of security information. Again, doing this will ensure that there is an effective security information system computerization. To achieve this, Visual Basic 6.0 is used for its implementation.

CHAPTER ONE

1.0 INTRODUCTION

National security is the requirement to maintain the survival of the state through the use of economic, security operatives especially police, political power and the exercise of diplomacy. The concept developed mostly in the United States of America after World War II focusing on the police and military might. Now, it encompasses a broad range of facets, all of which impinge on the police and military for economic security of the nation, lives property and values protected by national society. Accordingly, in order to possess national security, a nation needs to possess economic security, energy security, environmental security, etc. Security threats involve not only conventional foes such as other national states but also non-state actors such as violent non-state actors, narcotic cartels, multinational corporations and non-governmental organizations;

some authorities include natural disasters and events causing severe environmental change in this category.

The origin of the modern concept of "national security" as a philosophy of maintaining a stable nation state can be traced to the peace of Westphalia, wherein the concept of a sovereign state, ruled by a sovereign, became the basis of a new international order of nation states.

As an academic concept, national security can be seen as a recent phenomenon which was first introduced in the United States after World War II, and has to some degree replaced other concepts that describe the struggle of states to overcome various external and internal threats. The struggle of states to overcome various external and internal threats. The earliest mention of the term national security, however, was made in Yale University in 1790 wherein was made to its relation with domestic industries.

The concept of the national security became an official guiding principle of foreign policy in the United States when the National security Act of 1947 was signed on July 26, 1947 by the U.S. President Harry S. Truman. Together with its 1949 amendment, this act create American national security d important facets for American national security as the precursor to the department of defense, subordinated the security operatives branches to the new cabinet level position of the secretary of defense, established the National Security council and the Central Intelligence Agency. The Act did not define national security which was conceivably advantageous as it's ambiguity made it a powerful phrase to invoke whenever issues threatened by other interests of the state, such as domestic concerns, came up for discussion and decision making.

The realization that national security encompasses more than just security was present though understated, from the beginning itself.

The US National Security Act of 1947 was set up "to advise the president on the integration of domestic security and foreign policies related to national security".

Gen Maxwell Taylor's essay of 1947 titled "The Legitimate claims of National Security" has this to say;

The national valuables in this broad sense include current assets and national interests, as well as the sources of strength upon which our future as a nation depends. Some valuables are tangible and earthly; others are spiritual or intellectual. They range widely from political assets such as the Bill of Rights, National Security and political institutions and international relations to many economic assets which radiate worldwide from a highly productive domestic economy supported by rich natural resources. It is the urgent need to protect valuables such as these which legitimizes and makes essential the role of national security.

1.1 STATEMENT OF THE PROBLEM

Security information system has always played a vital role in the stability of a nation. Keeping security information manually can hinder some defense program and delay passage of security information to the appropriate body. Manual documentation of security information can lead to exposure of the information thereby creating threat to the nation at large. Hence, there is need for an automated security information system to guaranty safety of information.

1.2 OBJECTIVES OF THE STUDY

The general objective of the study is to develop a database for security information storage and retrieval.

Specifically, the following objectives are also considered:

i. To build a database system for police security information.

ii. To develop a software for managing security information.

iii. To determine the effectiveness of Nigerian police in managing signal.

1.3 DEFINITION OF TERMS/VARIABLES

Policing: Policing is another way of depicting the police.

Anti-policing: Anti-policing is the society's social attitude opposed to war between states and in particular countering arguments based on policism.

Databases: A systematically arranged collection of computer data, structured so that it can be automatically retrieved or manipulated. It is also called a databank.

National Security: The requirement to maintain the survival of the nation-state through the use of economic, policing, and political power and the exercise of diplomacy.

Information Security: means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction.

Classified Information is sensitive information to which the access is restricted by law or regulation to particular groups of persons.

Security Management is a broad field of management related to asset management, physical security and human resource safety functions.

CHAPTER TWO

LITERATURE REVIEW

2.1 SECURITY INFORMATION SYSTEM

System is the degree of protection against danger, damage, loss and crime. Security as a form of protection is structures and processes that provide or improve security as a condition. The Institution for Security and Open Methodologies (ISECOM) in the OSSTMM 3 defines security as a "form of protection where a separation is created between the assets and the threat". This includes but is not limited to the elimination of either the asset or the threat. Security as a national condition was defined in a United Nations study (1986) so that countries can develop and progress safely.

Security has to compare to related concepts: safety, continuity, and reliability, the key difference between security and reliability is that security must take into account the actions of people attempting to

cause destruction. Different scenarios also give rise to the context in which security is maintained.

With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarding in the interest of the national security.

Measures taken by a police unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness.

Perception of security may be poorly mapped to measurable objective security. For example, the fear of earthquakes has been reported to be more common than the fear of slipping on the bathroom floor although the latter kills more people than the former. Similarly, the perceived effectiveness of security measures is sometimes different from the actual security provided by those measures. The presence of security protection may even be taken for

security itself. For example, two computer security programs could be interfering with each other and even cancelling each other's effect while the owner believes he/she is getting double of the protection.

Security Theater is a critical form for the deployment of measures primarily aimed at raising subjective security in a population without a genuine commensurate concern for the effects of that measure on- and possibly decreasing- objective security.

Perception of security can also increase objective security when it affects or deters malicious behavior, such with the vital signs of security protections, such as video surveillance, alarm systems in a home, or an anti-theft system in a car such as Lojack, signs.

For example, approach a car, break the window, and flee in response to an alarm being triggered. Either way, perhaps the car itself or the objects inside aren't stolen, but with *perceived security*

even windows of the car has a lower chance of being damaged, increasing the financial security of the owner(s).

However, the non-profit , security research group, ISECOM, has determined that such signs may actually increase the violence, daring, and desperation of the intruder. This claim shows that perceived security works mostly on the provider and not the security at all. It is important, however, for signs advertising security not to give clues as to how to subvert that security, for example in the case whereby a home burglar might be more likely to break into a certain home if he or she is able to learn beforehand which company makes the security system.

Private security and public provide some of the same services and sometimes they even mirror each other, but there are distinct differences among the similarities. The scopes of their duties are different and each has advantages and disadvantages.

Allen Pinkerton (1855) established the first private police organization (Northwest Police Organization), by the end of the century, other organizations like Burns and Wackenhut were also established. Contact security guards were used heavily by industrial companies in the early part of the 20th century and were used as strikebreakers. In (1930), The Ford Motor Company had a private force of 3,500 called "The Ford Service". Private security is contracted services to companies, people or organizations for the protection of personnel and property. Private Security includes guard services, private investigators, bodyguards any detail (in house) detectives as also mobile patrols. All of these positions have the power of police on any property that is private or have an open contract. The reason behind this is because public police have no power or jurisdiction of any kind on private property. Police can't even go onto private property at all unless they have been invited on to that property by the owner and has the owners ok to be there. In almost all cases security need

some training and licensing, but fewer restraints than public police on the licensing and training.

America's law enforcement root can be traced back to English police models that were colonial times up until (1800's). in 1800 America experienced economic and social changes-industrialization, urbanization and immigration that forced changes in law enforcement making not just a local responsibility, but also a country, state and federal responsibility. This brought about forming the police department and jurisdictions, with New York being the first city to establish police force in 1844. Other social changes again forced changes in law enforcement-(1960s), civil right and the 1980s drug trafficking.

Public police are part of the government entity-local, country state or federal. All public police are based on a paramilitary model and have strict requirement, training and certification. Public police are

controlled by politics and government establishments, and restrained by laws and rules, but their role is the safety and welfare of the public.

Private security and public police have their advantages and disadvantages. Private security companies have less restrictions placed upon them, thus they can focus and effectively carry out their contracted duties. Private security also gets paid by performance and can negotiate salary. Also private security has more technical equipment available to them depending on the employer. The main disadvantage of private security personnel is lack of training or updated training and job retention, since they are salary employees they have less negotiation power than security and they do not get extra compensation for exceptional performance like security does. Police are also hampered by restrictions, legal and political; they are understaffed and outnumbered by security 10-1 and not accessible to

newer technology due to budget restraints and hiring limits. Police does not have advantage in training/advanced training and in job retention. Security on the other hand does not work off a budget and can buy whatever they want, update their technology any time they wish. Security can also pull its training from any source from government to private agencies.

In the corporate world, various aspects of security were historically addressed separately – notably by distinct and often non-communicating departments for IT security, physical security and fraud prevention. Today there is a greater recognition of the interconnected nature of security requirements, an approach variously known as holistic security, all hazards management and other terms.

Inciting factors in the convergence of security disciplines include the development of digital video surveillance technologies and the

digitization and networking of physical control systems. Greater interdisciplinary cooperation is further evidenced by the February 2005 creation of the Alliance for Enterprise Security Risk Management, a joint venture including leading associations in security (ASIS), information security (ISSA, the Information Systems Security Association), and IT audit (ISACA, the Information Systems Audit and Control Association).

In (2007) the International Organization for Standardization (ISO) released ISO 28000-Security Management Systems for the supply chain.

Although the title supply chain is included, this standard specifies the requirements for a security management system, including those aspects critical to security assurance for any organization or enterprise wishing to management the security of the organization and its activities. ISO 28000 is the foremost risk based system and is

suitable for managing both public and private regulatory security, customs and industry based security schemes and requirements.

2.2 INFORMATION SECURITY

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction, Julia H.(2001).

The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however there are some subtle differences between them.

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability

and correct operation of a computer system without concern for the information stored or processed by the computer.

Government, police, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

2.3 CIA AS INFORMATION SECURITY WATCHWORD

The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including: security network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science etc. For over twenty

years, information security has held confidentiality, integrity and availability (known as the CIA triad) to be the core principles of information security. There is continuous debate about extending this classic trio. Other principles such as Accountability have sometimes been proposed for addition-it has been out that issues such as Non-Repudiation do not fit well within the three core concepts, and as regulation of computer system has increased (particularly amongst the Western nations). Legality is becoming a key consideration for practical security installations.

Donn Parker (2002) proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, authenticity, availability, and utility.

The merits of the Parkerian hexad are a subject of debate amongst security professionals. Confidentiality is the term used to prevent the

disclosure of information to unauthorized individuals or systems. For example, a credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

In information security, integrity means that data cannot be modified undetectably. This is not the same thing as referential integrity in database, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security system typically provides message integrity in addition to data confidentiality.

For any information system to serve its purpose, the information must be available when needed. This means that the computing systems used to store and process the information, the security control used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to

power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks. In computing, e-Business and information security it is necessary to ensure that the data, transactions, communication or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are. In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

2.4 RISK MANAGEMENT IN INFORMATION SECURITY

A comprehensive treatment of the topic of risk management will be provided as well as some basic terminology and a commonly used process for risk management.

The CISA Review manual (2006) provides the following definition of risk management*. "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resources to the organization,* Vines (2003)". There are two things in this definition that may need some clarification. First, the process of risk management is an ongoing iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerability emerge every day. Second, the choice

of countermeasure (computer) (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). Vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (manmade or act of nature) that has the potential to cause harm.

The likelihood that a threat will use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called residual risk.

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use some qualitative analysis based on informed opinion, or where reliable dollar figure and historical information is available, the analysis may use quantitative analysis. When management chooses to mitigate a risk, they will do so by implementing one or more of three different types of controls. Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day to day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedure, standard and guidelines

that must be followed – the payment card industry (PCI) Data Security Standard required by Visa and Master Card is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies. Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestation of administrative control. Administrative controls are used for paramount importance. Logical controls are (also called technical controls) use software and data to monitor and control access to information and computing systems. For example, password, network and host based firewalls; network intrusion detection systems, access control lists, and data encryption are logical controls.

An important aspect of information security and risk management is recognizing the value of information and defining

appropriate procedure and protection requirements for the information. Not all information is equal and so not information require the same degree of protection. This requires information to be assigned a security classification. The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, developed a classification policy, the policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security control for each classification. Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important consideration when classifying information.

There are three different types of information that can be used for authentication: something you know, something you have, or something you are. Examples of *something you know* include such things as a PIN, a password, or your mother's maiden name. Examples of *something you have* include a driver's license or a magnetic swipe card. *Something you are* refers to biometrics. Examples of biometrics include palm prints, finger prints, voice prints and retina (eye) scans. Authentication requires providing information from two of three different types of authentication information. For example, something you know or something you have. This is called two factor authentications. On computer system in use today, the Username is the most common form of identification and the password is the most common form of authentication. Username and password has served their purpose but in our modern world they are no longer adequate. Username and password are slowly being replaced with more sophisticated authentication mechanisms.

To be effective, policies and other security controls must be enforceable and upheld. Effective policies ensure that people are held accountable for their actions. All failed and successful authentication attempts must be logged and all access to information must leave some type of audit trail.

2.5 THE RELEVANCE OF CRYPTOGRAPHY TO SECURITY INFORMATON

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptography key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the

information is in transit (either electronically or physically) and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signature, non-repudiation, and encrypted network communications. Older less secure applications such as telnet and ftp are slowly being replaced with more applications such as that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. Wired communications (such as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GnuPG or PGP can be used to encrypt data files and Email. Cryptography solutions need to be implemented using industry accepted solutions that have undergone rigorous peer

review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. PKI solutions address many of the problems that surround key management.

2.6 THE CONCEPT OF "DUE CARE" IN SECURITY INFORMATION

In the field of information security, Harris Shon (2003) offers the following definitions of due care and due diligence:

"Due care are steps that are taken to show that a company has taken responsibility for the activities that takes place within the corporation and has taken the necessary steps to help protect the company, its

resources and employees." And [Due diligence are the] "*continual activities that make sure the protection mechanism s are continually maintained and operational."*

Attention should be made to two important points in these definitions. First, in due care, steps are taken to show – this means that steps can be verified, measured, or even produce tangible artifacts. Second, in due care, there are continual activities – this means that people are actually doing things to monitor and maintain the protection mechanisms, and these activities are ongoing.

CHAPTER THREE

3.0 METHODOLOGY AND ANALYSIS OF THE EXISTING SYSTEM.

The existing system is manually carried out. Information on military signals is stored in an office file. Their personal data are being collected and each person has a file created for him or her.

Search on these files takes time. One has to go through the whole files in search of a particular record. This is cumbersome, hence the need for the computerization of the system.

3.1 FACT FINDING METHOD

Different methods adopted in the collection and gathering Data and Information for the project include, interview, Reference, and written texts.

3.1.1 INTERVIEW METHOD

This was done between the researcher and the Nigerian police authorities. Reliable facts were gotten based on the questions posed to them by the researcher.

3.1.2 REFERENCE TO WRITTEN TEXT

Security information documentations were studied and a lot of information concerning the system in question was obtained. Some forms that are necessary and available were assessed. Also internet downloads was made to obtain some text materials.

3.2 ORGANIZATIONAL STRUCTURE

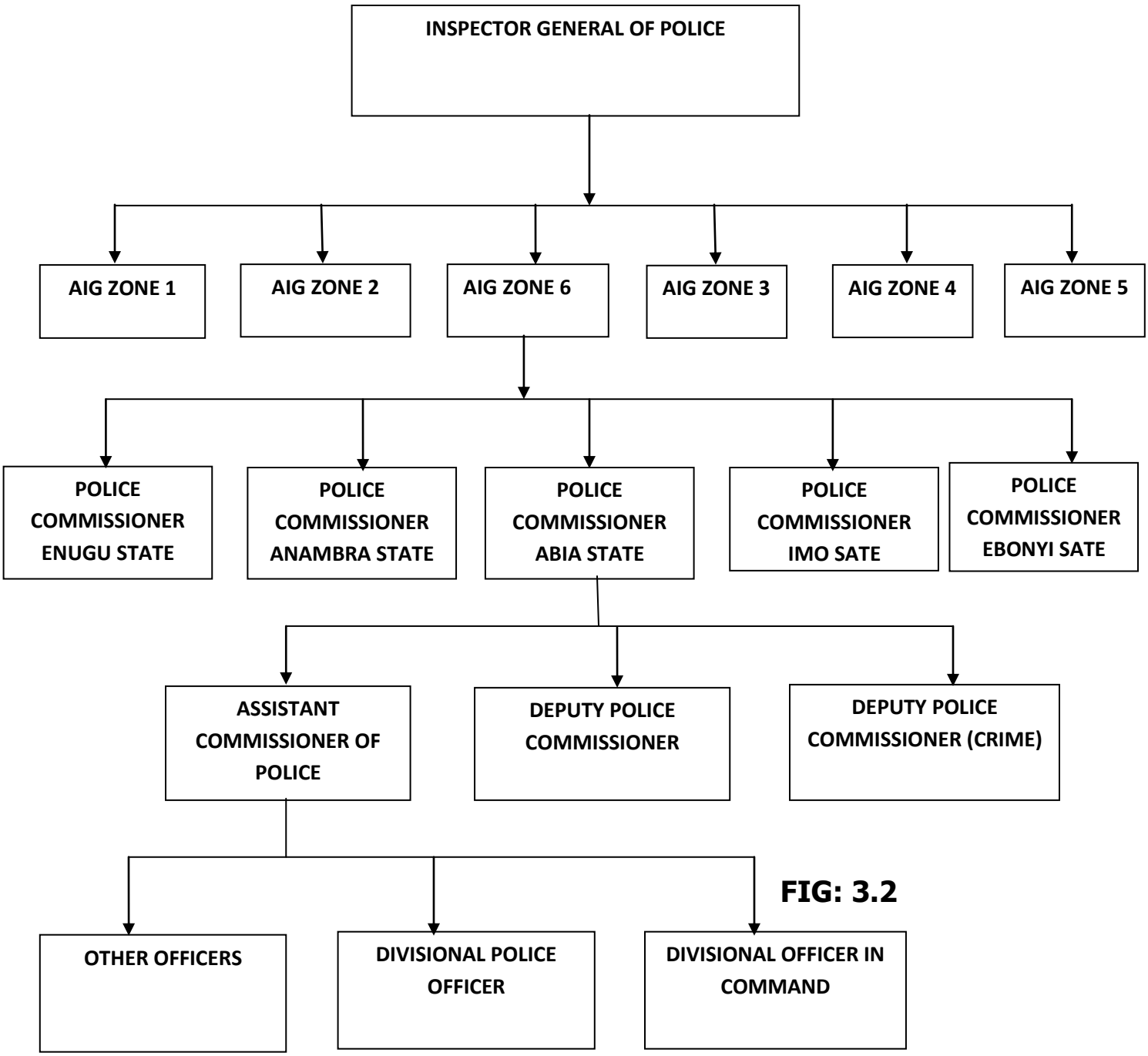


FIG: 3.2

3.3 OBJECTIVES OF THE EXISTING SYSTEM

The objective of the existing system includes:

- Collection of police personnel record
- Collection of security signals
- Opening a file for documenting these information
- Performing manual search on the file cabinet to retrieve information

3.4 INPUT, PROCESS AND OUTPUT ANALYSIS

3.4.1 INPUT ANALYSIS

The input to the system is the security information form. This form is used for recording security signals this forms the input to the system.

3.4.2 PROCESS ANALYSIS

The information gathered was processed into a more meaningful format for entry into the system. These personnel data are processed

to find out their areas of specialization and signal information sent out.

3.4.3 OUTPUT ANALYSIS

The output from the system is generated from the system inputs. More of the output generated is on personnel record, military signals, etc.

3.5 INFORMATION FLOW DIAGRAM

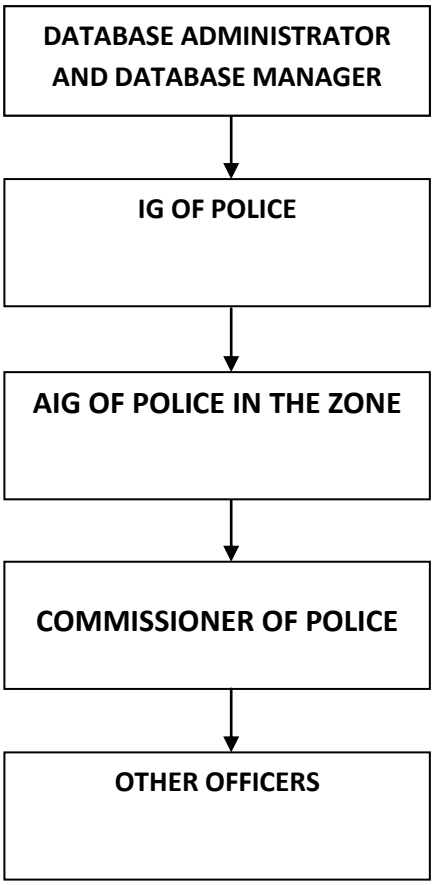


FIGURE 3.5 INFORMATION FLOW DIAGRAMS

3.6 PROBLEMS OF THE CURRENT SYSTEM

Manual system of operation faces a lot of problems which includes:

- Delay in data processing
- Errors in processing
- Loss of materials to fire incidents, termites / on transit
- Insecurity of data

3.7 JUSTIFICATION FOR THE NEW SYSTEM

The new system will help to solve all the problems inherent in the existing system. The justification for the new system includes:

- Timely processing of security information
- Error free processing of data
- Security of information is guaranteed
- Signal are received easily

CHAPTER FOUR

4.0 DESIGN OF THE NEW SYSTEM

4.1 Output Specification and Design

The output design was based on the inputs. The report generated gives a meaningful report to the management. The system designed generated the following reports.

1. Security Information Report
2. Police Report

These outputs can be generated as softcopy or printed in hard copy.

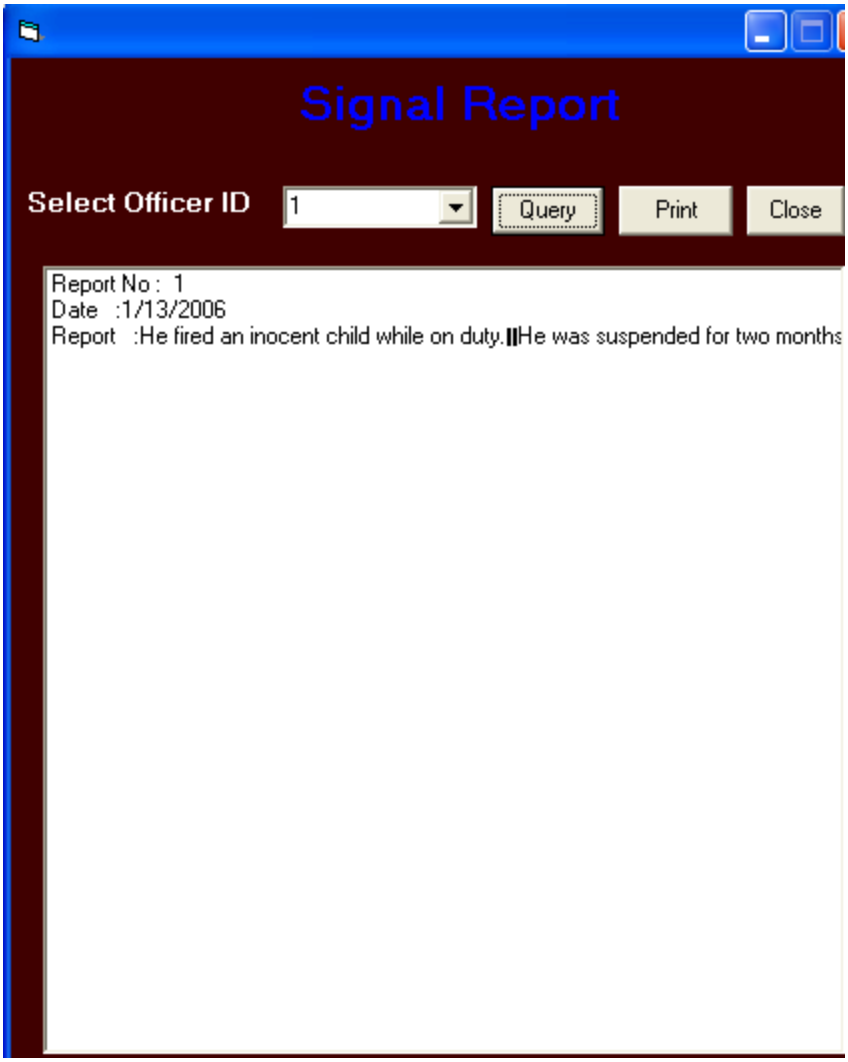
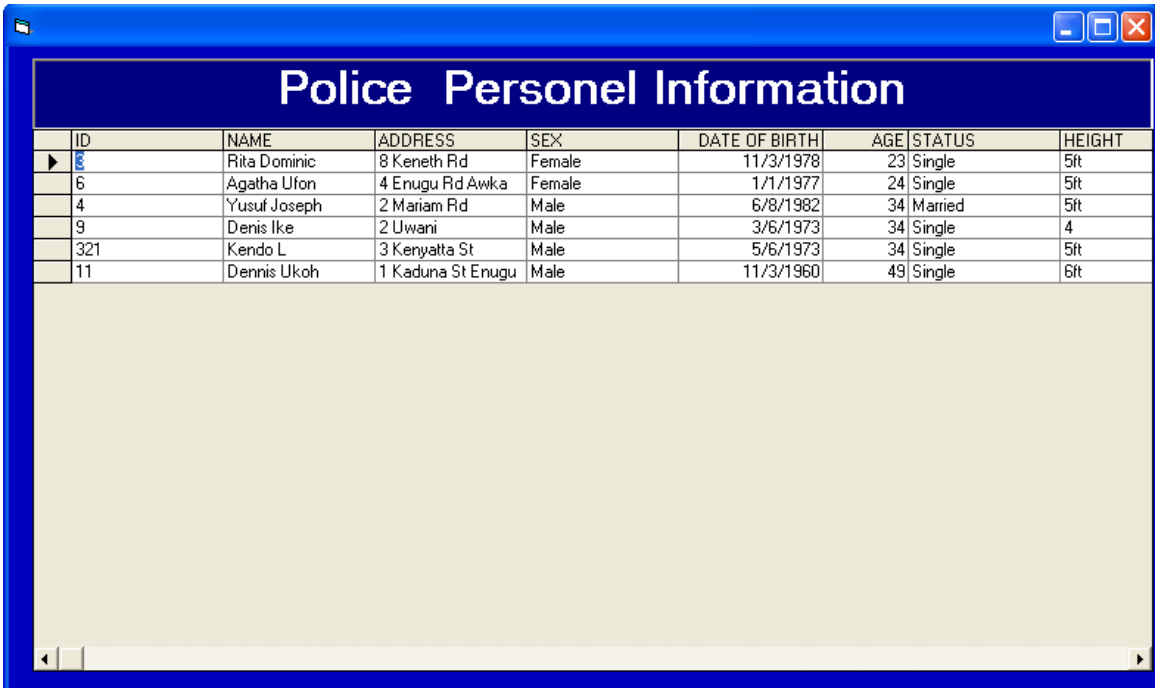


Fig: 4.1.1 Security Signal Report



Police Personel Information

ID	NAME	ADDRESS	SEX	DATE OF BIRTH	AGE	STATUS	HEIGHT
8	Rita Dominic	8 Keneth Rd	Female	11/3/1978	23	Single	5ft
6	Agatha Ufon	4 Enugu Rd Awka	Female	1/1/1977	24	Single	5ft
4	Yusuf Joseph	2 Mariam Rd	Male	6/8/1982	34	Married	5ft
9	Denis Ike	2 Uwani	Male	3/6/1973	34	Single	4
321	Kendo L	3 Kenyatta St	Male	5/6/1973	34	Single	5ft
11	Dennis Ukoh	1 Kaduna St Enugu	Male	11/3/1960	49	Single	6ft

Fig: 4.1.2 Police personnel information

4.2 Input Design and Specification

Computer is designed in such a way that sometimes it is call GIGO – denoting that what goes in is what comes out. The input forms are designs generally based on the necessary data that needs to be entered into the system. The data are captured through the keyboard and stored on a magnetic disk in an access database.

The new system is composed mainly of two input forms, they include:-

a) Police Personnel Information Form

b) Signal Form

Police Personnel Information Form

ID ----------

Name ----------

Address ----------

Date of birth ----------

Sex ----------

Age----------

Status ----------

Height ----------

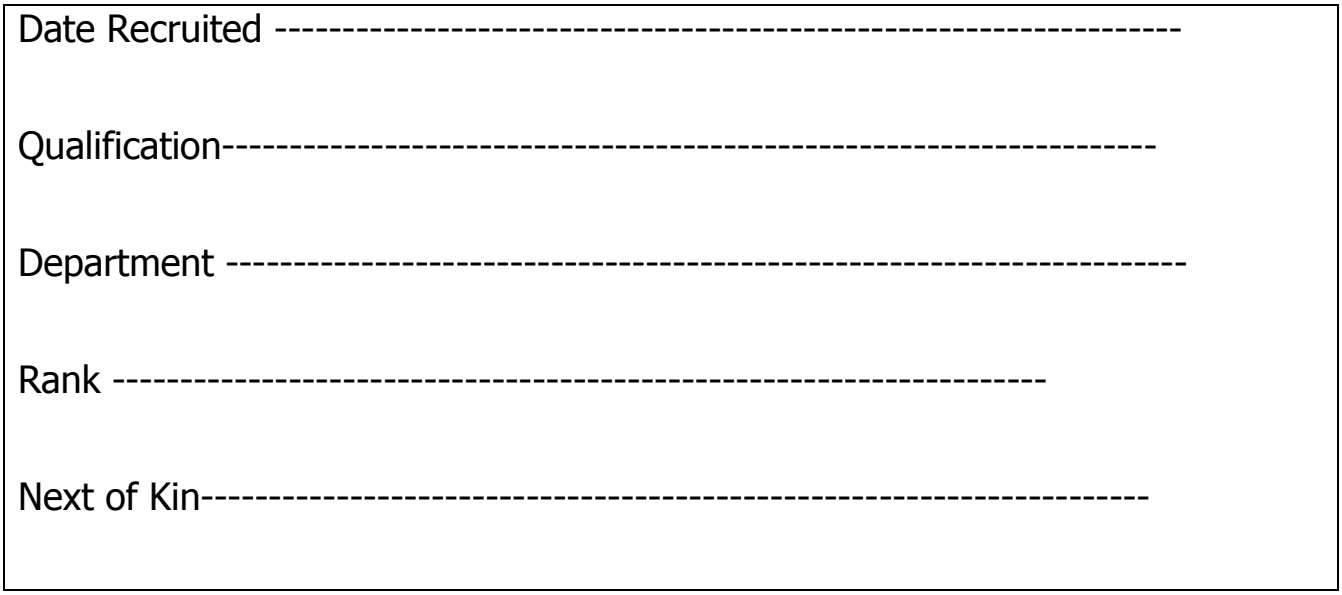


Fig: 4.2

4.3 File Design

The input to the system is stored in a database file. The design of file takes the format bellow.

Structure for File "Police Information"

Field Name	Data Type	Size
ID	Text	20
Name	Text	40
Address	Text	100
Date of Birth	Date\Time	8
Sex	Text	10
Age	Integer	2
Status	Text	20
Height	Text	10
Date Recruited	Date\Time	8

Qualification	Text	50
Department	Text	50
Rank	Text	30
Next of Kin	Text	50
Remark	Text	50

Table 4.3.1

Structure for File "Signal"

Field Name	**Data Type**	**Size**
ID	Text	20
Name	Text	40
Date	Date \ Time	8
Signal Report	Memo	0

Table 4.3.2:

4.4 Procedure Chart

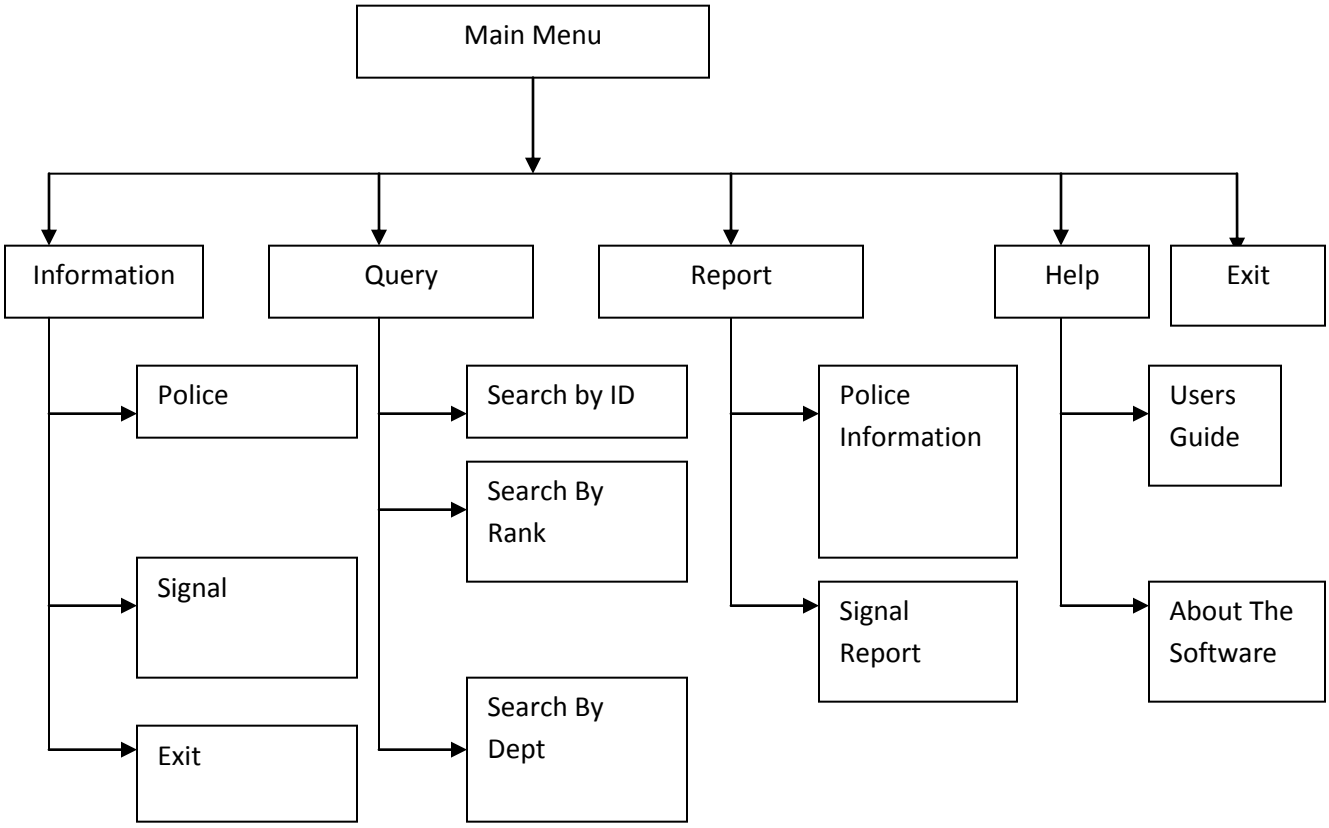


Fig 4.4

4.5 System Flowcharts

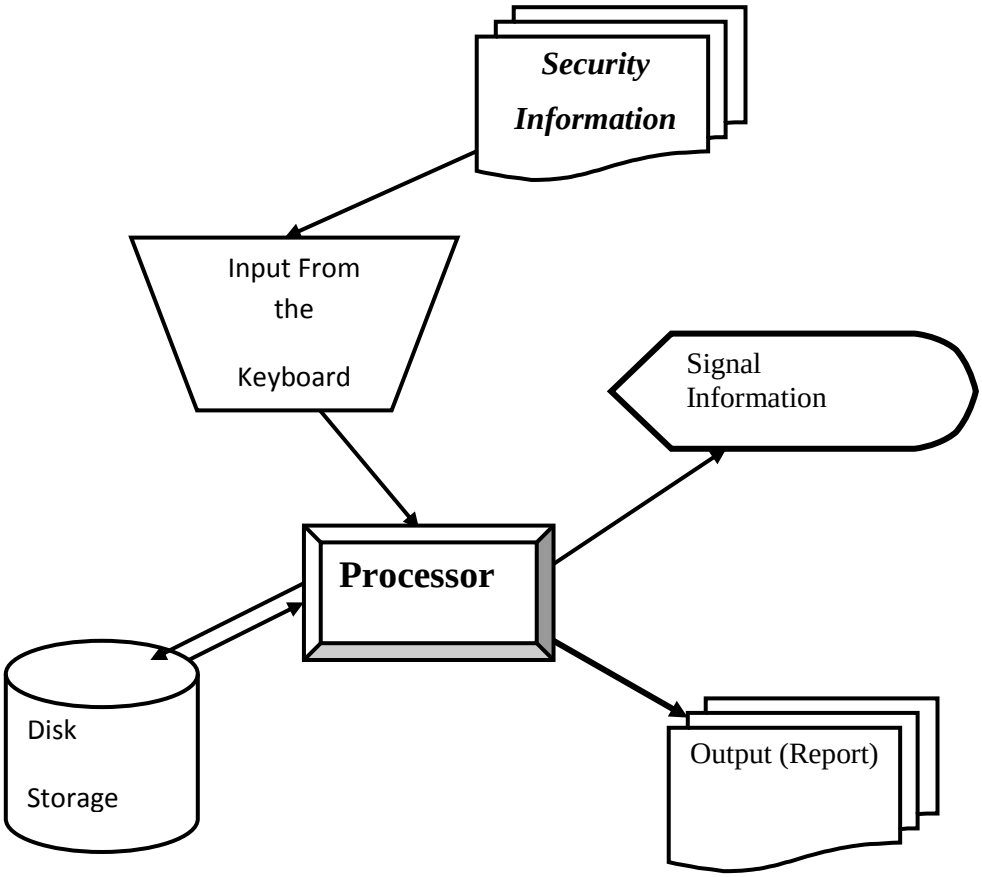


Fig 4.5

4.6 System Requirement

The requirements needed to implement this system are as follows:

4.6.1 Hardware Requirements

The software designed needed the following hardware for an effective operation of the newly designed system.

1. Pentium IV System.
2. The Random access memory (RAM) should be at least 128KB.
3. Enhanced keyboard.
4. At least 20GB hard disk.
5. E.G.A/V.G.A, a colored monitor.

4.6.2 Software Requirements

The software requirements includes:-

- A window 98 or higher version for faster processing
- Microsoft Access

- Visual Basic Version 6.0.

4.6.3 Operational Requirement

For the new system to be operational a conducive computer room has to be created and three computers installed for staff use.

4.6.4Personnel Requirement

A total of 2 computer operators are needed to manage the computer centre. They will oversee the entry of data into the system.

4.7 Program Flowchart

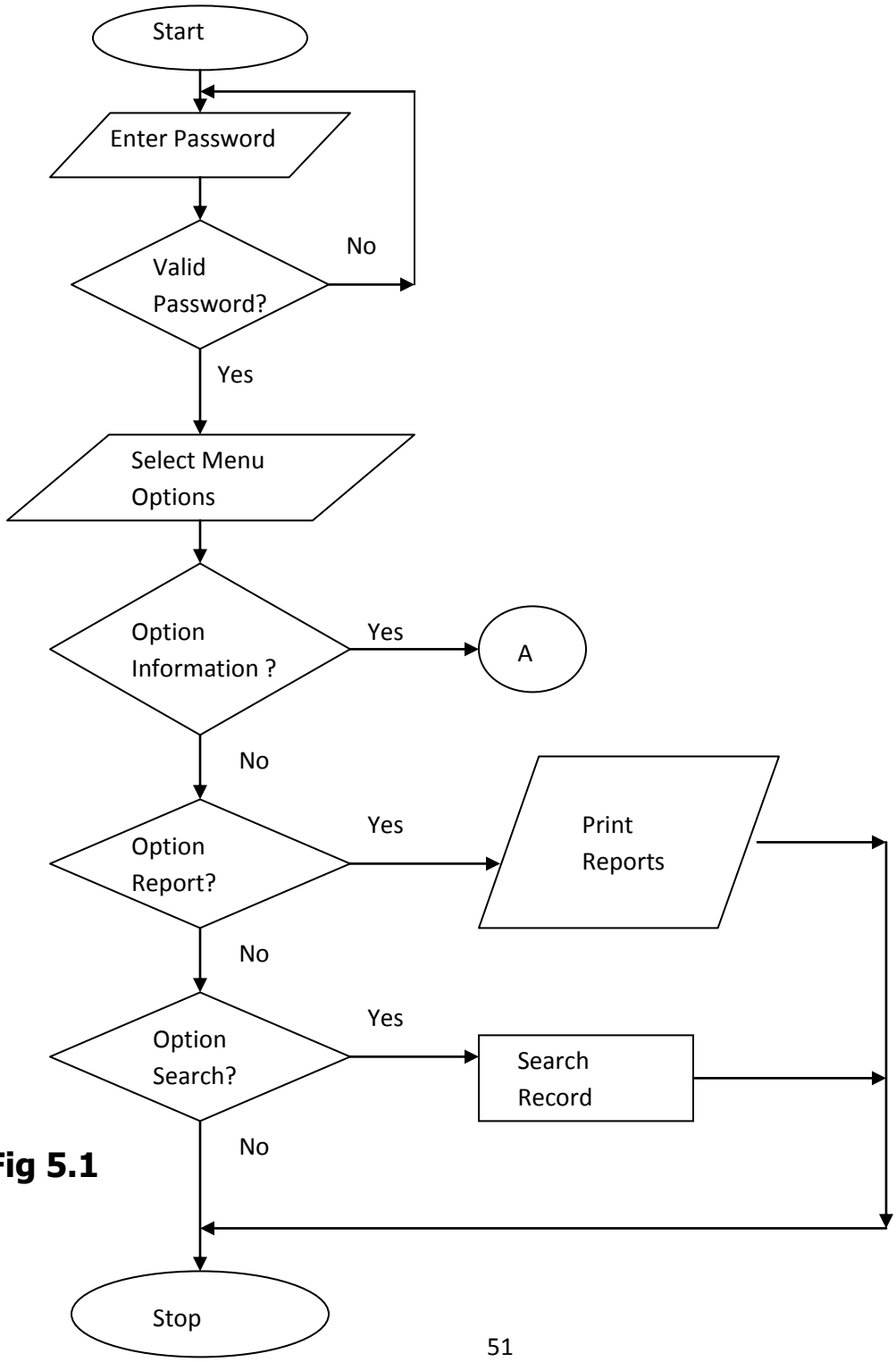


Fig 5.1

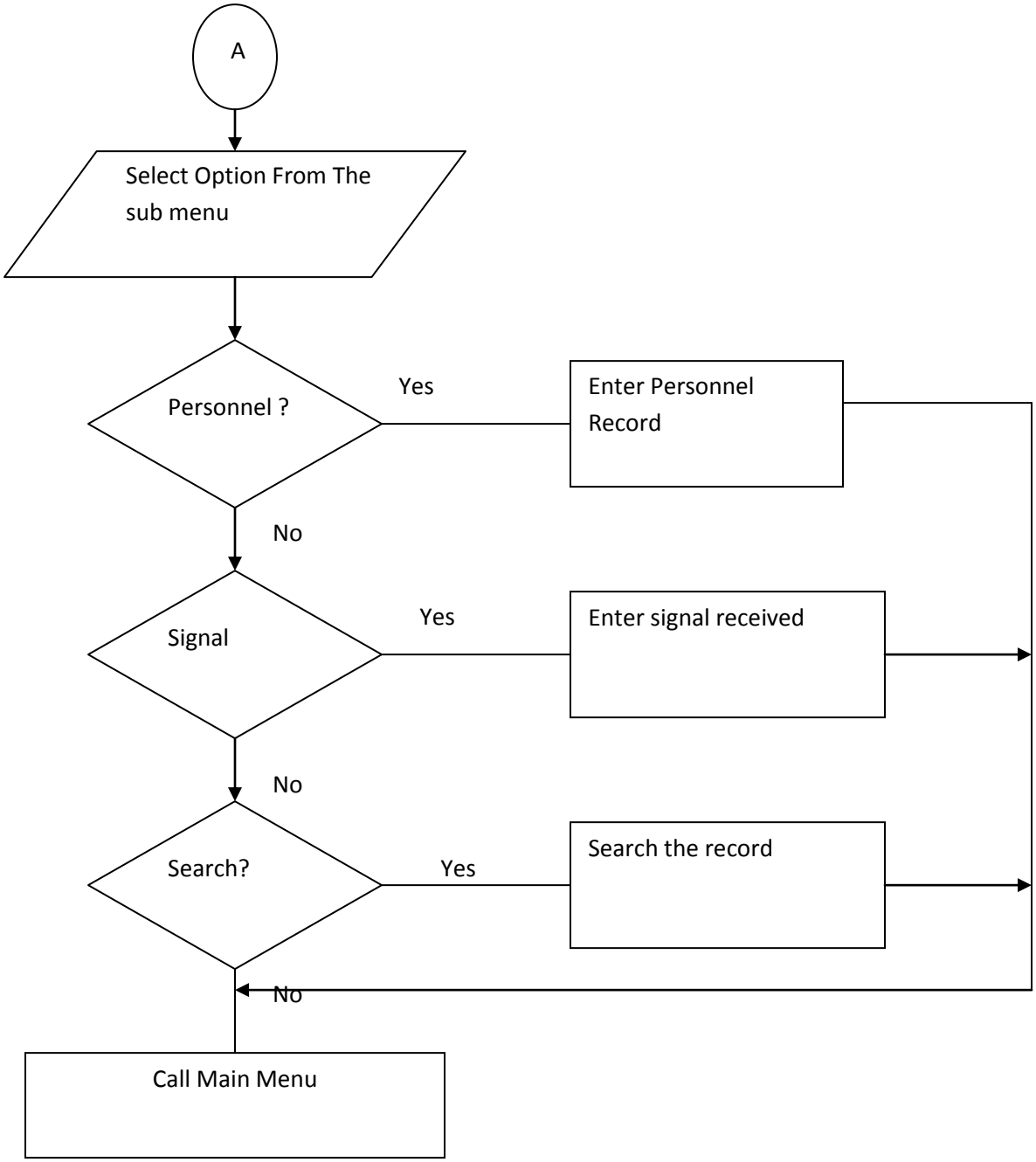

A
Select Option From The sub menu
Personnel ?
Yes
Enter Personnel Record
No
Signal
Yes
Enter signal received
No
Search?
Yes
Search the record
No
Call Main Menu

Fig 5.1.2

CHAPTER FIVE

SUMMARY, RECOMMENDATION AND CONCLUSIONS

5.1 SUMMARY

Information in its most restricted technical sense is an ordered sequence of symbols that record or transmit a message. It can be recorded as signs, or conveyed as signals by waves. Information is any kind of event that affects the state of a dynamic system. As a concept, however, information has numerous meanings. Moreover, the concept on information is closely related to motions of constraint, communication, control, data, form, instruction, knowledge, meaning, mental stimulus, pattern, perception, representation, and especially entropy.

The measures adopted to maintain national security in the face of threats to society has led to ongoing dialectic, particularly in the

liberal democracies, on the appropriate scale and role of authority in matters of civil and human rights.

Tension exists between the preservation of the state (by maintaining self-determination and sovereignty) and the rights and freedoms of individuals. Although national security measures are imposed to protect society as a whole, many such measures will restrict the rights and freedoms of all individuals in society. The concern is that where the exercise of national security laws and powers I not subject to good governance, the rule of law, and strict checks and balances, there is a risk that "national security" may simply serve as a pretext for suppressing unfavorable political and social views.

5.2 CONCLUSION

For much of police history the armed forces were considered to be for use by the heads of their societies, until recently, the crowned

heads of states. In a democracy of other political system run in the public interest, it is a public force.

The relationship between the police and the society it serves is a complicated and ever-evolving one. Much depends on the nature of the society itself and whether it sees the police as important, as for example in time of threat or war, or a burdensome expense typified by defense cuts in time of peace

5.3 RECOMMENDATION

The following recommendations are made:

That this system be implemented by Nigeria police to enable them go into computerized information system.

Also schools should expose students to some more relevant programming languages like visual basic so as to enable them carry out their projects on their own.

Libraries should b well equipped to simplify the work for the students and especially during the research phase.

These relationships are seen from the perspective of political police relations, the police industrial complex mentioned above, and the socio-police relationship. The last can be divided between those segments of society that offer for the police, those who voice oppositions to the police, the voluntary and involuntary civilians in the police forces, the populations of civilians in combat zone, and of course the police self-perception.

Police often function as societies within societies, by having their own police communities, economies, education, medicine and other aspects of a functioning civilian society. Although a police is not limited to nations in of itself as many private police companies (or PPC's) can be used or "hired" by organizations and figures as

security, escort, ot other means of protection where police, agencies, or militaries are absent or not trusted.

REFERENCES

Cynthia, A. (2008). *U.S. National Security*: A Reference Handbook. India: Pretience Hall. pp.223.

Depuy, T. N. (1992). *Understanding War*: History And Theory Of Combat. London:Leo Cooper Inc.

Kayode, F. J. (2003). *Governing The Security Sector in a Democratizing Polity*. Niger: Zed Books

MAIER, C. S. (1990). *Peace & Security For the 1990's*. New York Oxford Press.pp.132-134.

Olunsegun O. (1980). *My Command: An Account Of The Nigerian Civil war*. Ibadan: Heinemann Publishers:

Olusegun O. (2001). *Ambiguous Order: Police Forces in African States, Lynne Rienner*. Lagos: Longman Press.

Paleri, P. (2008). *National Security: Imperatives and Challenges*. New delhi: Tata McGraw-Hill.pp.321.

Romm, J. J. (1993). *Defining National Security*: The Non-military Aspects. Pew Project on America's Task in a Changed World (Pew Project Series). Council On foreign relations. pp. 122. California: Thompson Inc.

Scott, R. (1971). *The Nigerian Police London*: Methuen and Co.pp.332-333.

Taylor, G. M. (1974). *The Legitimate Claims o National Security*, Lacaste: Yehn Publishers.

Tucker, T. G. (1985). *Etymological Dictionary of Latin*. Chicago: Ares Publishers Inc. pp.112-114.

Yeun, F. (2006). *Human Security And The UN*: A Critical History, United Nations Intellectual History project (Illustrated ed.). Indiana University Press.pp.203.

APPENDIX

```
Private Sub Form_QueryUnload(Cancel As Integer, UnloadMode As Integer)
If UnloadMode<> 1 Then
MsgBox "Please exit from the File Menu", vbCritical
        Cancel = True
    End If
End Sub

Private Sub mnexit2_Click()
End
End Sub

Private Sub mnuAbout_Click()
MsgBox "This software is licensed to Nigeria Police"

End Sub
Private Sub mnuDetail_Click()
End Sub

Private Sub mnuEntry_Click()
```

```
End Sub

Private Sub mnubehaviour_Click()
frmbehaviour.cmbid.Clear
With frmrecuitment.memberdata
        .DatabaseName = App.Path& "\Reportsheet.mdb"
        .RecordSource = "select * from members"
        .Refresh
        .Recordset.MoveFirst
    Do Until .Recordset.EOF

frmbehaviour.cmbid.AddItem .Recordset.Fields("id")

        .Recordset.MoveNext

    Loop
    End With
frmbehaviour.ShowvbModal
End Sub

Private Sub mnubehreport_Click()
```

```
frmbehreport.cmbid.Clear
With frmrecuitment.memberdata
        .DatabaseName = App.Path& "\Reportsheet.mdb"
        .RecordSource = "select * from members"
        .Refresh
        .Recordset.MoveFirst
    Do Until .Recordset.EOF

frmbehreport.cmbid.AddItem .Recordset.Fields("id")


        .Recordset.MoveNext


    Loop
    End With
frmbehreport.list1.Clear
frmbehreport.ShowvbModal

End Sub

Private Sub mnudept_Click()
frmquery.Label1.Caption = "Select Dept"
```

```
frmquery.Optdept.Value = True
frmquery.cmbquery.Clear
frmquery.cmbquery.AddItem "Admin"
frmquery.cmbquery.AddItem "Engineering"
frmquery.cmbquery.AddItem "Information Unit"
frmquery.cmbquery.AddItem "Legal"
frmquery.cmbquery.AddItem "Account"
frmquery.cmbquery.AddItem "Production"
frmquery.ShowvbModal
frmquery.Dataquery.Refresh
frmquery.DBGrid1.Refresh

End Sub

Private Sub mnuExit_Click()
If MsgBox("Do you want to quit this application?", vbYesNo) = vbYes Then
MsgBox ("Thanks for using this application")
    End
End If
End Sub
```

```
Private Sub mnuManual_Click()
MsgBox "Contact the developer for users manual"
End Sub
Private Sub mnupolice_Click()
With frmreport.Datareport
        .DatabaseName = App.Path& "\Reportsheet.mdb"
        .RecordSource = "select * from members"
        .Refresh
   frmreport.DBGrid1.Refresh
    End With

frmreport.ShowvbModal
End Sub
Private Sub mnurank_Click()
frmquery.Label1.Caption = "Select Rank"
frmquery.optrank.Value = True
frmquery.cmbquery.Clear
frmquery.cmbquery.AddItem "Conel"
frmquery.cmbquery.AddItem "Captain"
frmquery.cmbquery.AddItem "Lt Conel"
frmquery.cmbquery.AddItem "Major"
```

```
frmquery.cmbquery.AddItem "Major General"
frmquery.cmbquery.AddItem "Group Captain"
frmquery.cmbquery.AddItem "General"
frmquery.cmbquery.AddItem "Brigadier"
frmquery.ShowvbModal
frmquery.Dataquery.Refresh
frmquery.DBGrid1.Refresh



End Sub

Private Sub mnurecruit_Click()
With frmrecuitment
.Show vbModal
End With
End Sub

Private Sub mnuSearch_Click()
frmquery.Label1.Caption = "Select ID"
frmquery.Optid.Value = True
frmquery.cmbquery.Clear
```

```
With frmrecuitment.memberdata
        .DatabaseName = App.Path& "\Reportsheet.mdb"
        .RecordSource = "select * from members"
        .Refresh
        .Recordset.MoveFirst
    Do Until .Recordset.EOF

frmquery.cmbquery.AddItem .Recordset.Fields("id")

        .Recordset.MoveNext

    Loop
    End With
frmquery.ShowvbModal
frmquery.Dataquery.Refresh
frmquery.DBGrid1.Refresh
End Sub



Private Sub cmdEnter_Click()
```

```
Static trial As Integer
Dim searchfound As Boolean
'comparing the password to give access or not

    If datLogin.Recordset.Fields("Password").Value = txtPassword.Text Then
searchfound = True
MsgBox("Access allowed, login succeeded")
trial = 1
        Unload Me
frmMainMenu.ShowvbModal
    Else
searchfound = False
MsgBox ("invalid password; enter your correct password")
        If searchfound = False Then
trial = trial + 1
        If trial > 3 Then
MsgBox ("Access denied, contact the administrator for correct password")
            End
        End If
        End If
txtPassword.Text = ""
```

```
txtPassword.SetFocus
End If
End Sub

Private Sub cmdExit_Click()
'end the program
End
End Sub
Private Sub Form_Load()
With datLogin
    .DatabaseName = App.Path& "\ReportSheet.mdb"
    .RecordSource = "select * from LoginTbl"
    .Refresh
End With
txtName.Text = "USER"
cmdEnter.Enabled = False


End Sub

Private Sub txtPassword_Change()
```

```
If txtPassword.Text<> "" Then cmdEnter.Enabled = True
End Sub

Private Sub cmdclose_Click()
With frmrecuitment
.Hide
End With
End Sub

Private Sub cmdsave_Click()
With frmrecuitment.memberdata
        .DatabaseName = App.Path& "\Reportsheet.mdb"
        .RecordSource = "select * from members"
        .Refresh
        .Recordset.MoveFirst
    Do Until .Recordset.EOF

            If frmrecuitment.txtid.Text = .Recordset.Fields("id") Then
MsgBox "The ID Number already exist"
GoTo 20
            Exit Do
```

```
            End If

        .Recordset.MoveNext

    Loop
    End With

With memberdata
        .DatabaseName = App.Path& "\Reportsheet.mdb"
        .RecordSource = "select * from members"
         .Refresh


    .Recordset.AddNew
    .Recordset.Fields("id").Value = frmrecuitment.txtid.Text
    .Recordset.Fields("name").Value = frmrecuitment.txtName.Text
    .Recordset.Fields("address").Value = frmrecuitment.txtaddress.Text
    .Recordset.Fields("sex").Value = frmrecuitment.Combsex.Text
    .Recordset.Fields("date of birth").Value = frmrecuitment.txtbirth.Text
    .Recordset.Fields("age").Value = Val(frmrecuitment.txtage.Text)
    .Recordset.Fields("status").Value = frmrecuitment.Combstatus.Text
```

```
    .Recordset.Fields("height").Value = frmrecuitment.txtheight.Text
    .Recordset.Fields("date recruited").Value = frmrecuitment.txtdate.Text
    .Recordset.Fields("qualification").Value = frmrecuitment.txtqaul.Text
    .Recordset.Fields("department").Value = frmrecuitment.combdept.Text
    .Recordset.Fields("rank").Value = frmrecuitment.Combrank.Text
    .Recordset.Fields("Proffesion").Value = frmrecuitment.txtkin.Text
    .Recordset.Update

End With


frmrecuitment.txtid.Text = ""
frmrecuitment.txtName.Text = ""
frmrecuitment.txtaddress.Text = ""
frmrecuitment.Combsex.Text = "Select Sex"
frmrecuitment.txtbirth.Text = ""
frmrecuitment.txtage.Text = ""
frmrecuitment.Combstatus.Text = "Select Status"
frmrecuitment.txtheight.Text = ""
frmrecuitment.txtdate.Text = ""
frmrecuitment.txtqaul.Text = ""
frmrecuitment.combdept.Text = "Select Department"
```

```
frmrecuitment.Combrank.Text = "Select Rank"
frmrecuitment.txtkin.Text = ""
20
End Sub


Private Sub Form_KeyPress(KeyAscii As Integer)
frmPassword.Show
frmPassword.txtPassword.SetFocus
'frmMainMenu.Show
Unload Me
End Sub


Private Sub Timer1_Timer()
frmPassword.Show
frmPassword.txtPassword.SetFocus
'frmMainMenu.Show
Unload Me
End Sub
```

```
Private Sub Command1_Click()
frmreport.PrintForm
End Sub

Private Sub Command2_Click()
frmreport.Hide
End Sub
Private Sub Command3_Click()
frmreport.Datareport.Recordset.Delete
End Sub
Private Sub Form_Load()
With datLogin
    .DatabaseName = App.Path& "\ReportSheet.mdb"
    .RecordSource = "select * from LoginTbl"
    .Refresh
End With
txtName.Text = "USER"
cmdEnter.Enabled = False



End Sub
```