REPORT ON IMPLEMENTATION

OF

A SECURED TRANSACTION REGISTRY

IN

BANGLADESH

BY: Phyllis Raymond

Assisted By:

Dr. Ananya Raihan

Taneem M. R. Islam

A. K. M. Fahim Mashroor

Mohd. Asaduzzaman

Faisal Saeed

TABLE OF CONTENTS

Executive Summary

In order to stimulate the economy of Bangladesh, small- and medium-sized enterprises (SMEs) need to be able to improve and expand their operations. In order to do that they need access to credit. The current credit-lending situation in Bangladesh does not provide for security of the lenders in lending money using movable goods as collateral.

The lenders have no mechanism at this time to perfect a security interest in goods that were used as collateral in a loan for unincorporated businesses that include the majority of the SMEs. Also they have no way of establishing priority in relation to other creditors. Plus the only mechanism that creditors have in the situation of default is to initiate a long, costly and somewhat ineffective court process to recover the monies owed. Often the court process takes so long that the goods are no longer of any value when sold at a judicial sale.

Lenders are reluctant to lend money to SMEs because of the lack of security. Often lenders will require immovable property as collateral on a loan. As is common in all countries, both developed and developing, the smaller businesses do not own immovable property. In New Brunswick, Canada 85% of businesses do not own immovable property but prefer to operate out of leasehold premises.

For the above reasons, JOBS, with the assistance of Project Consultant, Allen Welsh, has introduced a draft Secured Transactions Act to the Government of Bangladesh. This legislation would provide a more secure lending environment in Bangladesh. The Act provides for a Secured Transaction Registry that would allow lenders to establish perfection and priority in moveable goods when those goods are being used as collateral. The legislation also provides for immediate recourse by the lender at the time of default. The lender can seize the goods and sell them without first having to go through the courts. Banks, leasing companies and other interested parties are potential clients of a Secured Transaction Registry.

The Ministry responsible for the administration of the Secured Transaction Registrar's office will be determined by parliamentary procedures when the legislation is entered. The Registrar's office, established within government, would be responsible for overseeing the operation of the Registry and introducing any required regulatory changes to government. The Secured Transaction Registry will be an electronic registry where clients are responsible for the entry and retrieval of information from the Secured Transaction Database.

Since the Government of Bangladesh does not have the expertise or infrastructure to fully administer the Registry, it is recommended that the Government hire a private sector company to act as an agent of government for administration purposes. The Government of Bangladesh would maintain ownership of all hardware and software components of the Secured Transaction Registry system.

The private sector agent would be responsible for the administration of the Business Office and the operation of the Secured Transaction Registry. The Business Office would be the client contact point for the Registry. Clients would be financial institutions, leasing companies, etc. Those people who access the system are users under a client account. Through the Business Office clients can establish an account and deposit monies on their account set up for Registry usage. The Business Office would be responsible also for the Client Helpdesk, Hardware, Software and Database Maintenance. The Business Office will be responsible for providing account status information to clients, revenue accounting to the Registrar of the Secured Transaction Registry, statistical information regarding volumes of transactions and revenues received and the remittance of funds to the government.

The Secured Transaction Registry will consist of two components: the Client Database and the Secured Transaction Database component. The Client Database will provide services as described above. The Secured Transaction Database is the electronic registry on which clients will enter notices of new charges (referred to as enlistments in the legislation), continuations, amendments, and terminations of existing charges. The

Registry will also provide a search capability to the client. The search capability will allow the searcher to query under debtor name to establish if there are any previous charges involving a particular debtor or goods. The Registry system will provide reports to clients on the details of registrations and searches.

By building the Client Database Component as a separate component to the Registry, a foundation will be established for other e-commerce applications to be developed by the Government of Bangladesh. The Client Database can act as the gateway to other applications providing client support, transaction and revenue tracking facilities, and statistical and accounting information on the operation of the system or systems attached to the Client Database.

Documentation must be prepared to support the system. The documentation required are user guides as well as system operation and maintenance manuals to ensure the smooth, uninterrupted operation of the system. In advance of implementation of the system a training program must be undertaken and training manuals produced for that purpose.

It is recommended that the Secured Transaction Database be established as an internet accessible system. Clients will need to install desktop software on their workstations to access the system.

Security and integrity of the database are of utmost importance to the sustainability of the Secured Transaction Registry. Great care must taken in selecting the software and hardware to support the Registry. The hardware selected must ensure security, and integrity of the system. System capacity must also be taken into consideration. It is recommended that additional servers be put in place to mirror the application servers. The additional servers will ensure uninterrupted service to the clients in the event of a failure of the primary servers.

Established Secured Transaction Registry software should be obtained from a third party vendor to support the Secured Transaction Registry. Many discussions have taken place

around whether the software should be developed in Bangladesh or whether an existing software package should be purchased. There are several reasons for suggesting that procurement of an existing software package would be the best option. The computerized registry must be operational at the time of implementation of the legislation and the system must be operating on a stable environment. An existing software package will be able to be installed quickly without considerable delay and will have been proven as a stable operating system on a specified hardware environment. The cost of software procurement can be deferred, with the software suppliers charging a per transaction fee as transactions are completed on the system. Should the software be developed in Bangladesh, the Government would be required to pay the up front cost for system development before realizing any revenues from the system.

A business plan has been prepared for the Secured Transaction Registry. Expected transaction volumes have been based on information provided by the Bangladesh Bank, and discussions with the banks and leasing companies. The Business Plan took into consideration the cost of hardware, training, software development/procurement, office setup costs, and hardware and software maintenance costs. From projected volumes and costs a fee structure was developed. It is felt that the fees to perform a transaction on the Secured Transaction Registry should remain low so as not to cause a further burden on the borrower who will eventually be charged the transaction fees by the creditor.

Based on figures provided by the Bangladesh Bank and other financial institutions, volumes estimates were established. Three volume estimates were established; optimistic, conservative and moderate volumes. The moderate volume amounts were determined to be the most realistic. Based on moderate volume estimates of just new enlistments (175,000) during the first year it was estimated that the revenue received calculated at $5 per enlistment for just new enlistments would be $875,000.

Costs were then taken into consideration. It was estimated that the Hardware and Operating software would cost $443,200. The procurement cost of the Secured Transaction component software is estimated at $1,000,000 including training and

documentation costs. After calculating projected revenues, setup and ongoing costs, it is estimated that the Secured Transaction Registry will recover all costs by year 3 of operation and at the end of year 5 be able to realize a cumulative income of $3,197,341.

1. INTRODUCTION

A. The Present Credit Situation In Bangladesh

The economy of Bangladesh is dependent on jobs, investment and trade nationally and internationally. Small and medium sized enterprises (SMEs) could assist in development of a stronger economy.

Almost every study or report on economic development from most developing nations states that the SMEs (small- and medium-sized enterprises) of any given country have become the engines that drive developing economies. These reports broadly say that governments need to enable SMEs by enacting laws that will help to motivate business activity and preserve fairness in commerce. In Bangladesh, the potential growth of SMEs is constrained or restricted in a number of ways. In other words, SMEs are suffering here because the legal and regulatory environment does not promote commerce and in fact, in some cases, this environment even acts as a hindrance to business growth.[1]

The financial institutions are reluctant to lend money to small businesses using movable goods as collateral. The main reason for the reluctance is the lack of legal procedures to "perfect" and enforce a security interest in movable goods. When credit is extended, interest rates can range from 14 per cent per annum to 22 per cent, or more, per annum. The high interest rates are due to the uncertainty of the financial institution being able to recover the loan should default occur. In order to seize goods from a defaulter, a financial institution must now follow the long process of taking the defaulter to court. This process can take years to complete. All the while the collateral decreases in value at a steady rate.

Bangladesh gained independence in 1971. Since that time, progress has been made toward economic reforms and poverty is declining. Despite the economic reforms,

[1] Moveable Asset Financing and Its Legal Implications in Bangladesh – Roger Bird, JOBS, USAID, May 30, 2001.

Bangladesh remains one of the world's poorest, most densely populated and least developed nations. The government of Bangladesh has made some headway improving the climate for foreign investors. Progress on other economic reforms has been slow because of opposition from interest groups.

Why has Bangladesh remained one of the world's poorest countries? Part of the answer to that question lies in the lack of empowerment that the Government of Bangladesh has given to its people and SMEs to improve current situations. Without access to credit, individuals and SMEs cannot gain the necessary money to move forward in the business community. In order for SMEs to increase the workforces, invest in products and trade both nationally and internationally, credit must be available. Presently credit is available to businesses that have immovable property (land and buildings) to be used as collateral or to businesses who are well-established bank clients. Many of the SME's do not own immovable property. This case holds true in developed countries. It has been stated that 85% of the businesses in New Brunswick, Canada do not own immovable property. In New Brunswick most businesses operate out of leasehold premises.

The solution to the problem is to enact the Secured Transactions law that allows SME's to use movable goods as collateral to gain credit. This legislation would also allow creditors to seize goods in the event of default without having to go through the lengthy and costly court processes and judicial sale. This legislation will create a win/win situation for all involved.

B. Existing Bangladesh Registry System

There is presently a mechanism in place within the Joint Stocks Registry system for financial institutions to register notices of security interests in movable goods owned by incorporated companies. The process is slow. According to the lenders it can often take up to three weeks to be notified whether or not the registration will be accepted, and wrought with delays at every level resulting in additional costs. There is another registry available for registering security interests in ships, but again the registry is used for loans

given to incorporated companies. These registry systems in place result in segmented reporting on security interest in moveable goods. The registry systems in place do not cover all parties who receive credit or all assets. The only debtors listed in the existing registries are incorporated companies.

SMEs are commonly not incorporated, therefore, the financial institutions have no venue to register notice of a security interest in movable property owned by SMEs or search for prior security interests. As well there is no registry available to give notice of security interests in goods owned by individuals. Without a mechanism allowing for the establishment of perfection and priority of security interests in moveable goods owned by SMEs and individuals, the insecurity of financial institutions extending credit to these parties is increased. The financial institutions have no comfort level in the knowledge that they will be able to recover value for loans if a default should occur or that their priority will be established. In order to correct these weaknesses the Secured Transactions Act, 2001 was proposed to the Government and includes the establishment of a collateral registry for movable assets. It is for that purpose that a Secured Transaction Registry in Movable goods is being proposed for Bangladesh.

C. What is a Secured Transaction Registry?

The Secured Transaction Registry is a database, either electronic or in hard copy, in which Secured Creditors (Financial Institutions, Leasing Companies and Private Lenders) can give notice of their security interest in the movable goods of an enterprise or individual. The author of this report is recommending a fully electronic Secured Transaction Registry be implemented. The Secured Transaction Registry also provides for the creditor to establish priority of the security interest. According to legislation the general rule with a Secured Transaction Registry is first registered security interest in the collateral has first priority. The Secured Transaction database is also available for interested parties to search (query) to find if there are prior security interests in goods pledged by a debtor.

D. Purpose of the registries of secured transaction

In the most simplistic of terms, the purpose of a Secured Transaction Registry is for Secured Parties to perfect their security interest and to establish priority of their security interest in the movable goods of the borrower, lessee, etc. In most situations the Security Interest must be enlisted in the Secured Transaction Registry in order to be perfected.[2] The first registered interest, in most cases, has priority over subsequently registered security interests.

The reason for perfecting and setting the priority of a security interest is to give notice to subsequent purchasers and/or secured parties of the existence of a security interest. As an explanation: A purchaser may search (query) a debtor name on the database to ensure that a security interest does not exist in the goods that they are interested in purchasing. According to the proposed legislation, if someone should purchase goods to which a security interest is attached the purchaser has also purchased the security interest (debt). It is in the best interest of each purchaser to ensure that the goods that they are about to purchase are free of prior security interests registered by another party.

Subsequent lenders should also search the Secured Transaction Registry to ensure that there are not prior security interests registered on goods which are to be used in collateral in a loan that they are going to provide to a borrower. If security interests on the collateral exist the lender will take their place in line of the creditors according to date and time of registrations, with the first registered interest having priority.

E. Legal Framework for Sustaining a Secured Transaction Registry System

JOBS, with the assistance of Project Consultant, Allen Welsh, has introduced a Secured Transactions Act to the Government of Bangladesh. This Secured Transactions Act provides for the establishment of the Registry, establishes the rules for perfection and

[2] Secured Transactions Act, 2001 – Chapter II – Perfection and Priority of Charges – – Sections 12 & 13.

priorities and gives the Secured Creditors a means of recourse should the debtor default on a loan.

The method of recourse, under the new Act, is substantially different from that in practice in Bangladesh today. Since there is no method of perfection and establishment of priority for Secured Transactions with SMEs, the Creditor, upon default, must apply to the court to have their security interest validated. This court process can be very lengthy resulting in years of time elapsing between the default and the judicial sale. The courts have an appeal process available to the debtors that can further delay the process. Often collateral will fall into disrepair during this time due to lack of routine cleaning and maintenance. Collateral can become valueless during the court process resulting in a loss to the creditor.

Under the proposed Act, the creditor must perfected a security interest by registering (enlisting) their notice on the Secured Transaction Registry. Once the security interest has been perfected, the creditor can immediately seize the goods from the debtor without having to go through the courts. This allows the creditor to expedite the process of seizure and sale while ensuring the amount of depreciation is kept to a minimum.

F. Government Organizations and Private Institutions Interested in Registering Secured Transactions

Registration of secured transactions is of interest to financial institutions and leasing companies that are likely to be the primary clients of the Secured Transaction Registry. The purpose of a Secured Transaction Registry is to maintain a database accessible by any party interested in verifying security interests in moveable goods.

Lawyers and notaries usually also play a role in the process of securing transactions. They may intervene directly in the process of registration or act on behalf of creditors or debtors to verify property rights. They necessarily will be clients of the search (query) function of the Secured Transaction Registry (searching information on collateral securing transactions). Furthermore, any individual interested in verifying security interests in collateral is a potential client in the search process.

Therefore, the main clients of the Secured Transaction Registry will be:

- commercial banks and their branches, including foreign trade banks, credit organizations and other financial companies;
- leasing companies;
- local law firms;
- offices of the notary public;
- government ministries, departments and agencies responsible for lending to debtors who use moveable goods as collateral;
- government ministries enforcing tax claims, judgements, etc.
- other interested parties who want to search the registry to verify security interest.

2. WHERE SHOULD THE SECURED TRANSACTION REGISTRY RESIDE WITHIN THE GOVERNMENT OF BANGLADESH

While interviewing potential clients of the Secured Transaction Registry, the questioned was posed on what branch of the Government of Bangladesh should be responsible for the administration of the Secured Transaction Registry. The common response was with the Bangladesh Bank responsible to the Ministry of Finance. To every individual questioned, this appeared to be the natural placement of the Registry in the government. Reasons given for the response was that the Government needed to be responsible for the registry, however, government involvement should be minimized. In addition there appears to be a certain confidence in the Bangladesh Bank. By placing the responsibility with the Bangladesh Bank, the Registry would remain controlled by the Government but at arms length from Government. That being said, the Ministry ultimately made responsible for the operation of the Registry will be determined by parliamentary procedures.

Staff required within the Government to administer the Secured Transaction Registry will consist of:

- Registrar of the Secured Transaction Registry

- Deputy Registrar of the Secured Transaction Registry
- Receptionist
- Office Assistant.

Please see Section 11 – The Business Plan for set up costs for the Secured Transaction Registry Office within the Government of Bangladesh.

3. OPTIONS FOR THE ADMINISTRATIVE STRUCTURE OF THE REGISTRY

In discussing how the Secured Transaction Registry should be operated in Bangladesh, the team was presented with three options:

Option 1:The government would administer the system directly signing up clients to the Secured Transaction Registry.

Option 2: The government will submit a Request for Proposal to single licensees who would be responsible for the Secured Transaction Registry with branch offices of that licensee throughout the country.

Option 3: The government would submit a Request for Proposal to any companies interested in acting as an agent for government in the administration of the Secured Transaction Registry.

Option 1: The government would administer the operation of the Secured Transaction Registry

Discussion: In discussions with government officials and potential clients of the Secured Transaction Registry, it is apparent that both parties want as little government involvement as possible. The Government of Bangladesh does not have the expertise, staff or the infrastructure at present to fully support a Secured Transaction Registry as envisioned in this report. The onus would be on the government, in this case, to provide client support, maintain the database, accept payments on client accounts, etc. This would increase the workload of government and increase the involvement of government

and possibly place the government in a risk of liability should a staff member be responsible for an error or omission on a client account that would affect an enlistment.

Conclusion: For the above-mentioned reasons this option is not considered viable.

Option 2: A single licensee would administer the operation of the Secured Transaction Registry from branch offices throughout the country of Bangladesh.

Discussion: The single licensee must have the expertise to administer the Secured Transaction Registry from a central office and branch offices throughout Bangladesh. Those branch offices would provide registration and searching services on behalf of all of the clients. In discussions it was pointed out that there is not one company in Bangladesh with branch offices in all of the divisions of the country. Along with the knowledge that there is no one company with branches of all areas of the country, it was further determined that no one company has the expertise required to administer the Secured Transaction Registry. By allowing one company to become the sole entity to register and search on the Secured Transaction Registry, the government would be creating a monopoly. The financial institutions that have been interviewed have indicated that they would like direct access to the Secured Transaction Registry so that they can conduct their own registrations and searches.

Conclusion: For above-mentioned reasons, this option is not viable.

Option 3: A single licensee would administer the operation of the Secured Transaction Registry issuing client accounts to financial institutions, etc. throughout the country

Discussion: The licensee should be capable of administering the Client Database consisting of client setup, accepting payments, etc. The licensee may, according to terms and conditions of the license agreement with the Government, subcontract to database administrators, helpdesk administrators, training consultants and software developers. The software developers do not necessarily have to be from Bangladesh. The software package could be one that has already been developed for another Secured Transaction Registry in another jurisdiction. The budget discussion in Section 11 – Business Plan, will outline the estimated cost of buying an existing software application. The software developers will have to work closely with the administrators of the other functions of the Registry whether developed within the country or purchased from an outside source. The fact that the licensee subcontracts other functions should be transparent to the clients of the system and to the Government of Bangladesh.

The licensee would have to guarantee that there were clients in every division of Bangladesh who could register and search on behalf of interested parties. These clients could be law offices, financial institutions, etc. who would offer a value adder service to interested parties.

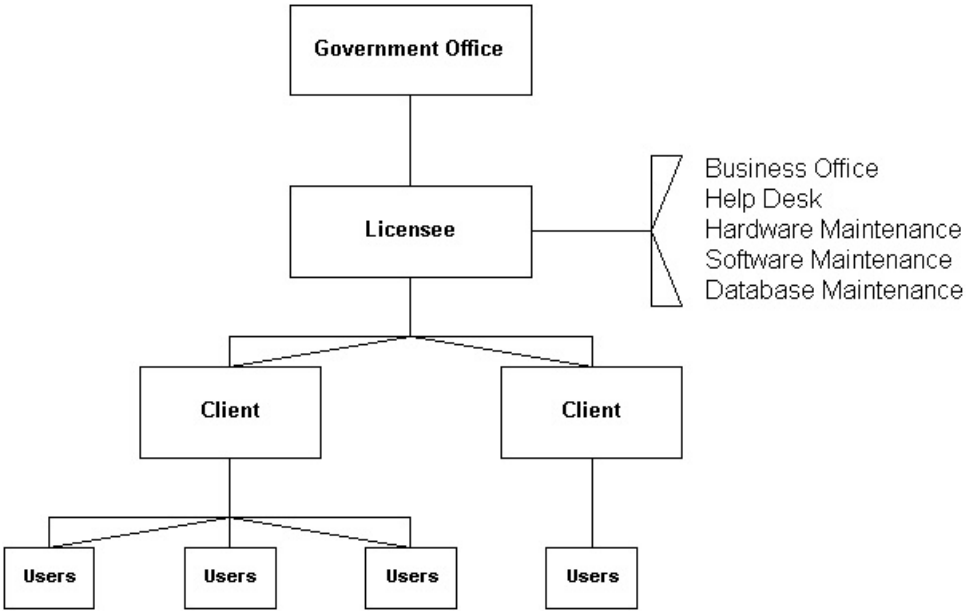
Conclusion: This option is the most viable. The Government of Bangladesh will sign a contract with the Licensee authorizing the licensee to act as an agent on behalf of the government and, subject to approval by the Government of Bangladesh, to subcontract any necessary functions and maintenance of the Secured Transaction Registry. Should the licensee subcontract any tasks associated to the Secured Transaction Registry, the licensee must provide the names of the parties to which the tasks will be subcontracted and the terms and conditions of the contract between the licensee and the subcontractor. The Government of Bangladesh must indicate approval of the above mentioned contract before the licensee enters into the subcontract with another party. All contact with the Government will be through the licensee. The use of a private sector licensee and private sector subcontractors will stimulate the private sector economy of Bangladesh. This option will also enable their subcontractors to develop expertise in the area of e-

commerce. The Government of Bangladesh is encouraging e-commerce within the country.

Under this arrangement the Government of Bangladesh will be the owner of the Secured Transaction Registry software and all hardware used for the development, operation and maintenance of the Registry. The hardware owned by the Government of Bangladesh must include all production and development servers and the attached peripherals. The software developer will write a software change proposal for every change to be made to the system. The software change proposal will detail the new functionality or changes to existing functionality and what modules of the system will be affected. The estimated cost of the change will also be included in the software change proposal. The Registrar of the Secured Transaction Registry will review the proposed changes to the system and the costs associated. Before any changes can be made to the system the Registrar must first indicate approval in writing to the licensee.

Figure 1 shows the organizational structure of the Secured Transaction Registry.

Figure 1



4. COMPONENTS OF THE SECURED TRANSACTION REGISTRY

Working on the assumption that Option 3 in Section 3 of this report would be implemented in structuring the administration of the Secured Transaction Registry, the components of the Registry have been designed as detailed below.

The Secured Transaction Registry will consist of two main components:

A. Client Database
B. Secured Transaction Database

Establishing the Registry as two separate components will build the foundation to be used for other e-commerce applications. Once established the Client Database can act as a gateway to other electronic applications introduced by Government. The Client Database will already be developed to handle client administration, revenue accounting and transaction tracking. This same functionality may be used by future applications such as an electronic Land Registry or Motor Vehicle Registry.

A. Client Database Component

The Client Database will consist of the client set up, tracking and account management component of the Secured Transaction Registry. Client accounts will need to be established with the capability of creating multiple users under one account with multiple roles (See Documentation Section 6 (A) – Client Account Agreement). A financial institution may have many users of the system under a client account established for the financial institution. Each of those users may have different roles. There must be one, and only one, administrative user in each client account. This administrative user will have the capability to activate and revoke another user's rights under the same client account. Each user of the account will be given an access role to the system. A user may be given the capability to only search (query) the Secured Transaction database. Another user may only be given registration (enlistment) capabilities. While a third type of user may be given registration and search capabilities. The Administrative user will be given

full capabilities on the system including functions that are not available to all other users in the client account. This may include:

- Activating and revoking other users permissions on the system;
- Identifying the roles of the other users and acting as the main contact with the system administrators to alter the role of a user (to either increase or decrease user capabilities);
- Signing electronic checks to replenish the amount in the client account, should that functionality be made available.
- Acting as the main contact to whom the system administrators will report any problems with other users within the client account or ask any questions concerning that specific client account;
- Initiating a Global Change should that functionality be introduced into the Secured Transaction Database. The administrative user will be the only user under a client account who will have that capability. See the description of the Global Change feature in the Secured Transaction Database descriptions.

The client accounts should be predeposit accounts, in which the client deposits an amount of money. The basic Client Database should have the capability of entering the predeposited amounts to a client account. Eventually the capability of accepting credit card payments, electronic checks and electronic funds transfers can be added to the Client Database. As the client uses the system, the fees for the transactions performed will be deducted from the predeposited amount. All users within a client account, which has a negative balance, should be stopped from performing registrations and searches.

The Client Database must track all activities associated to client accounts and users under a client account. It must track all payments to and expenditures from an account. It must track all enlistments and searches associated to a client account down to the user level within the account. A Secured Party number must be created for each client account. Use of the Secured Party number will enable the system to take the name and address of the client account from the Client Database and

populate the Secured Party fields in the Secured Transaction Database Component. Association of the Secured Party Number will facilitate the Global Change feature.

The Client Database must have the capability of reporting statistics such as volumes of transactions performed and fees collected for those transactions from any point in time to another. The Client Database must also be able to report to a client the status and the balance of the client account along with the fees collected for any transactions performed by the client account. The client account reports must be capable of reporting on the overall client account as well as down to the user level i.e. how many transactions a user under a client account performed and what fees were charged for the transactions. The Client Database must be capable of providing full accounting reports to the Registrar of the Secured Transaction Registry. These reports must provide information on the financial transactions and the volumes of each registration and search activity. It must also provide the Registrar with full financial reporting on the revenues received on behalf of the government and the transfer of those fees to the Government.

Conversely the Client Database Component must attach a client account number and user ID to each transaction so that when a transaction needs to be tracked to retrieve the registrant information, the information can be tracked to the specific client and user within that client account. Neither a client account nor users can be deleted from the Client Database component, as all transactions performed on the Secured Transaction Registry must be tracked to a client account and user under that account.

Online help text must be created for the Client Database component for section and field level help to assist the user in understanding the requirements of the various forms and functionality of processes. Edit checks and associate error messages must be developed to alert the user to requirements and system problems.

Clients will be required to install desktop software on each workstation that will be used for accessing the Secured Transaction Registry. To recover just the costs of developing the desktop software it is suggested that the clients be charged for each copy required.

B. Secured Transaction Database Component

The Secured Transaction Database Component must allow for several features. They include:

Required Features

i. Entry of a new enlistment
ii. Continuation of an existing enlistment
iii. Amendment of an existing enlistment
iv. Termination of an existing enlistment
v. Registration Number (check digit)
vi. Search by debtor name (Enterprise or Individual)
vii. Search by a Unique Identification Number (in the case of an individual debtor)
viii. Search by registration number
ix. Reports verifying the details of the entry of new enlistments, continuations, amendments, terminations, re-enlistments, global changes and search results including the selected details of matches to be included in the search result report.
x. Historical Tracking of Enlistments
xi. Help Text and Error Messages
xii. Broadcast News

Optional Features

xiii. Re-enlistment of an lapsed or recently terminated enlistment
xiv. Global Change
xv. Batch Uploading of Files
xvi. Search by Serial Numbered Vehicle

The following is an explanation of the above noted functions in greater detail:

NECESSARY FEATURES

i. Registration of a new enlistment

The registration of a new enlistment allows the registrant to enter basic elements of the notice. The term of the enlistment will automatically be 5 years or, if the registrant specifies, a longer period. The term entered must never be less than 5 years. The details of the name and address of debtor(s) (in the case of a debtor who is an individual, the Unique Identification Number of each debtor*), name and address of the secured party(s), general collateral description, serial numbered vehicles description(s) and additional information. The general collateral description and additional information sections should allow for free form entry of the information. All other sections should have specific fields of entry. The Additional Information section can be used to describe immovable property to which crops and fixtures that are subject to a security interest are attached. In the case of addresses, picklists should be made available for street types, place, district, division and country names to facilitate entry. The serial numbered vehicles section should include a picklist of collateral type defined as serial numbered vehicles under the legislation. Edit checks must be built into the system to ensure that the minimum requirements of an enlistment have been entered. Once the enlistment is submitted to the database, the registrant will be presented with a registration number and a verification statement report must automatically be produced. The verification statement must show all details of the registration entered.

The enlistment or continued enlistment must remain accessible to the enlistment officer for a period of 5 years beyond the lapse date. That does not mean that the information relating to those enlistments must remain searchable for 5 years from the lapse date. The enlistments can be archived to another medium after a period of one year from lapse date.

A method must be developed by which the enlistment officer can retrieve those lapsed enlistments from the archive medium.

*NOTE: It has been brought to the attention of this author that there are many individuals in Bangladesh who bear the same name. All individuals must be uniquely identified on the system. In order to be able to identify a specific debtor, it is suggested that the Tax Identification Number be associated to each debtor individual name. (See the section on Searching by Unique Identification Number and Appendix C for a description of the use of the Tax Identification Number.)

ii. Continuation of an existing enlistment

Continuation of an existing enlistment allows a registrant to extend the term of an enlistment. The term must be extended for at least 5 years from the current expiry date of the enlistment. A continuation can only be done within one year prior to the expiry of the enlistment. Under the legislation the continuation function can be accessed through the entry of the registration number of the enlistment and the Secured Party name.* Once a continuation of an enlistment has been submitted to the database, a report known as a verification statement must be produced showing all of the details of the enlistment history as well as the old and new expiry dates.

The enlistment or continued enlistment must remain accessible to the enlistment officer for a period of 5 years beyond the lapse date. That does not mean that the information relating to those enlistments must remain searchable for 5 years from the lapse date. The enlistments can then be archived to another medium after a period of one year from lapse date. A method must be developed by which the enlistment officer can retrieve those lapsed enlistments from the archive medium.

*NOTE: The requirement of entering the Secured Party name should be reviewed. In some existing systems, the entry of the registration number of the enlistment will allow the registrant to review the first entry in each section of the enlistment to ensure that the enlistment is, in fact, the one to be continued.

iii. Amendment of an existing enlistment

Amendment of an existing enlistment allows the registrant to amend everything about the original enlistment and subsequent amendments except for the term. The amendment function allows the registrant to add, change or delete any information concerning the debtor, secured party, general collateral description, serial numbered vehicles description and/or additional information. The system must track all changes made to the registration never deleting any information completely from a record. When a piece of information is added by a new enlistment or an amendment the registration number of either the original or amendment, as the case may be, must be reported with the item of entry. A change of information will be treated as an add and delete. For example: If a debtor was added by the original registration and deleted by an amendment, the column beside the debtor name should show under the added heading the original registration number and under the deleted column the registration number of the amendment. All additions and deletions of information must be associated to the registration number by which the addition or deletion was made. There must be an edit check on the system to ensure that not all debtors, secured parties or collateral is removed from the enlistment. In order for the enlistment to remain valid there must be at least one remaining debtor, secured party and item of collateral listed in the notice. Once the amendment is submitted to the database, a verification statement of the amendment must be produced showing the details of what was accomplished in the amendment including all additions and deletions. Each verification statement must include the history of the enlistment from the date of the original enlistment to date. That includes any continuations or other changes that have occurred until the amendment was submitted. Also, if any client other than the Secured

Party has registered an amendment to an enlistment, notice of that amendment must be sent electronically to the Secured Party or by mail in the form of a report call Notice to Secured Party Report. The client, if receiving the notice electronically, must be notified that there is a notice available the next time they sign on to the system. If the Secured Party is not a client of the system, the Registrar of the Secured Transaction Registry must produce those reports in hard copy and mail them to the Secured Parties. Those notices, which must be mailed, will be sent electronically to the Registrar of the Secured Transaction Registry on a daily basis. The legislation again requires the registration number and secured party name to retrieve the enlistment for amendment purposes. (See the note at the end of Continuation of an existing enlistment.)

iv. Termination of an existing enlistment

Termination of an existing enlistment allows the registrant to fully terminate (discontinue) an existing enlistment. The enlistment should remain searchable on the system for 30 days after termination. Partial termination of an enlistment will be accomplished by using the Amendment of an Existing Enlistment feature where one of the debtors or part of the collateral is deleted from the enlistment. The legislation again requires entry of the registration number and the secured party name to retrieve the enlistment for termination purposes. (See the note at the end of Continuation of an existing enlistment**.)** If someone other than the Secured Party terminates an existing enlistment, the Notice to Secured Party must be produced in the same manner as mentioned in the Amendment of an Existing Enlistment section. To encourage Secured Parties to terminate registrations where all obligations of the debtors have been met there will be no fee for the registration of a termination.

v. Registration Number (check digit)

The registration number must be produced in consecutive order incorporating a check digit at the end. (Please see Appendix B for the explanation of the use a check digit and the formulas for calculation taken from the Web Site of the International Association of Corporation Administrators.) Use of a check digit further reduces the requirement of

entering the Secured Party name when accessing an enlistment for the purposes of Continuation, Amendment, Termination and Re-enlistment. It is strongly recommended that a check digit be incorporated in the registration number. The Wohler's Double Digit Deluxe Check Number further reduces the chance of transposition errors in entering registration numbers.

vi. Search by debtor name (Enterprise or Individual)

Search by debtor name allows a person, entering a query, to search under the name of an individual or the name of an enterprise. All exact matches to the name of an individual must appear in the search selection index. The search selection index should contain the name of the individual and the location (place name) from the address file associated to that debtor. From the index a searcher must be able to drill down to view the details of the registrations in which they are interested. A search report must be able to be generated where the searcher can include any and/or all of the details of the enlistments in which they are interested. All details of the chosen enlistments must appear on the search result report. The enlistment office must supply to any interested parties details of the existing of enlistments within the previous 3 days and no earlier than the previous 3 days. As provided in the legislation, the search functionality should allow a searcher to enter the date of the search within the previous 3 days, but not earlier than the previous 3 days, from search date. The search result report must also show the number of matches to the search criteria. The search result report must also show the number of the enlistments appearing in the search selection index which were included and which were excluded from the report.

A search of a debtor enterprise name should act in the same manner as described above. The only addition to the functionality for an enterprise name search is that noise words (common business terms) should be removed from the search string and a search of the enterprises should be conducted on a key word search of the remaining words in the enterprise name. Noise words are words that are commonly used in the name of an enterprise i.e. Enterprise, Company, Co, Limited, Ltd. etc. (See Appendix D for a list of

the Noise Words supported by the International Association of Corporation Administrators (IACA)).

vii. Search by Unique Identification Number in the case of an individual debtor

The author of this report has been made aware of the fact that there are several individuals in Bangladesh who bear the same name(s). It is for that reason that an additional functionality is recommended for the system to be implemented in Bangladesh. One of the options for uniquely identifying an individual is the Tax Identification Number. (See Appendix C for the description of a Tax Identification Number). It is for that reason that an addition of the search by Unique Identification Number function is recommended for the system. The entry of every debtor individual name should be linked to a Unique Identification Number. When searching under the Unique Identification Number the searcher will be able to retrieve only matches associated to the Unique Identification Number and the individual associated to it. This, in the case of commonly used names, will significantly reduce the search selection index returned as the result of entering criteria. The criteria used in the Unique Identification Number search will be just the unique identification number. It will return in a search selection index a list of exact matches to the Unique Identification Number, the name of the individual associated to that number and the location (place name) of that individual. Again the searcher must be able to drill down to the details of each and every registration shown in the search selection index. The search result report will function as described in the above section on debtor name searching.

viii. Search by registration number

A search conducted on a specific registration number need not produce a search selection index as one, and only one, registration should exist on the system with that unique number. When a searcher enters a registration number as criteria the details of the registration must be presented to the searcher on the system. The searcher can then choose whether or not to produce a search result report including all of the details of that registration.

ix. Reports

Reports will be used for verifying the details of the entry of new enlistments, continuations, amendments, discharges, re-enlistments, and global changes. A searcher may choose to produce search result reports including the details of selected matches to be included. All search result reports produced by a searcher must be copied to CD-ROM or Optical Disk. All reports must be sent to the registrant/searcher electronically. See the section on Amendment of Existing Enlistment and Termination of an Existing Enlistment regarding the production and distribution of the Notices to Secured Parties.

x. Historical Tracking of Enlistments

The history of an enlistment must be shown on the system when a user accesses the original enlistment or any subsequent enlistments (continuations, amendments, terminations, global changes, re-enlistments, etc.). This history of the enlistment family must show from the date the original was entered until the user accesses any enlistment within that enlistment family.

xi. Help Text and Error Messages

Help Text must be developed for the system to inform registrants and/or searchers of the requirements and functionality of sections of the Registry. The help text should be accessible from field and section level of each enlistment and search function. The Batch uploading of a file feature does not include help text.

Edit checks must be incorporated in the Secured Transaction Database to ensure that minimum requirements for an enlistment exist when the registrant submits a notice. An error message will appear if the minimum requirements are not met stopping the registrant from submitting the notice until all requirements have been met. On many systems edit checks are placed at various areas in the enlistment and searching processes

as a helpful hints. The resulting error messages do not stop the registrant from continuing with the submission.

xii. Broadcast News

Broadcast News is the functionality used to notify users of changes to legislation affecting the system, changes to system functionality and planned system outages. An example of a use of Broadcast News is to notify users that the system will be shut down during normal operating hours to make upgrades. The Broadcast News should not be on a menu where someone may choose to select it. Broadcast News must appear automatically when the user accesses the system.

OPTIONAL FEATURES

xiii. Re-enlistment of a lapsed or recently terminated enlistment

Re-enlistment of a lapsed or recently terminated enlistment allows the registrant to bring the enlistment back on the system within 30 days of lapse or termination. In the case of a lapsed enlistment, re-enlistment will bring the notice back on the system for 24 hours within which time the registrant must register a continuation. In the case of a terminated enlistment, re-enlistment will bring the notice back on the system for the remainder of the existing term.*

*****NOTE: This functionality is not mentioned in the draft legislation but is desirable as anyone can access the system, if they have a client account, and terminate an enlistment. The system should also allow for the re-enlistment of a termination that has been done in error so that the Secured Party will not lose the priority standing of the enlistment.

xiv. Global Change

Global Change is the function that allows a full assignment of enlistments from one Secured Party to another, in one step, or to change the name and/or address of a Secured

Party. In order for a Global Change to affect an enlistment, the Secured Party Number must be associated to the enlistment on original entry of the Secured Party information. The administrative user, and only the administrative user, will be able to access the Global Change functionality. The restriction of that functionality, to just the administrative user, is done for the security reasons. The administrative user, in order to assign all enlistments from one secured party to another, will access the Global Change functionality and assign the enlistments by entering the assigning secured party number and the receiving secured party number. In order to change the name and/or address of a secured party, the administrative user would first have the name and/or address changed on the client account and related secured party information. The administrative user would then access the Global Change functionality and assign the enlistments from the secured party number associated to the enlistments to the same secured party number. Global Change is a batch process that is done while the system is off line. The next day a report will be sent electronically to the registrant and to the Secured Party, if not the same as the registrant, identifying the registration numbers of the enlistments which were affected by the Global Change and showing the registration number of the Global Change.

xv. Batch Uploading of Files

Batch uploading of files allows the registrant to create of file containing multiple enlistments and/or searches off line and then upload the file to the Secured Transaction Database in one process. The file must be created in a set format that will be acceptable to the Secured Transaction Database. A manual must be created to define the requirements for setup of the files. Unlike on-line registrations, the enlistments and/or searches do not occur immediately. The file must wait in a queue where it is picked up by a processing computer and processed by the system. The batch uploading process affects the Client Database, as does every other enlistment and search performed on the system. The system will track all enlistments and searches processed from the batch file and deduct the fees from the client account accordingly. As the registrant is not interactively entering the searches, a search result report is automatically produced for

each search contained within the batch file. As with the entry of all enlistments, and registrations related to existing enlistments, a verification statement will automatically be produced.

xvi. Search by Serial Numbered Vehicle

Search by serial numbered vehicle allows a person entering a query to search under the serial number of serial numbered vehicles, as defined in the legislation. The search selection index must contain all matches associated to the serial number entered as criteria. From the index a searcher must be able to drill down to view the details of the registrations in which they are interested. A search report must be able to be generated where the searcher can include any and/or all of the details of the enlistments in which they are interested. All details of the chosen enlistments must appear on the search result report. The search result report must also show the number of matches to the search criteria. The search result report must also show the number of the enlistments appearing in the search selection index which were included and which were excluded from the report.

NOTE: Although this functionality is not necessary for the initial implementation of the Secured Transaction Registry, if this functionality may be introduced in the future, the Serial Numbered Vehicle information should be kept separate from the General Collateral descriptions. Serial numbered vehicles should, in order to be searchable in the future, separate the serial numbers into separate tables from the General Collateral descriptions.

5. SYSTEM ENHANCEMENTS

Every computer program in existence today is subject to future enhancements. Changes to legislation, upgrades to operating systems and the supporting software result in the need for enhancements to the system. As part of the five-year plan for the operation and maintenance of the Secured Transaction Registry, an amount to cover the cost of

enhancements must be included in the budget. Nonurgent system enhancements should not be implemented one at a time. Instead nonurgent system enhancements should be bundled in a package (release). Each release must be accompanied with instructions to the system maintenance team detailing the files to be affected, the processes and procedures for implementation and the functionality of the changes being made. These instructions will be included as an addendum to the Operations Manual (See Documentation - Section 6(**G) -** Operations Manual). Before nonurgent enhancements are developed and implemented a Software Change Proposal should be completed. The Software Change Proposal will detail what changes are to be made, what modules will be affected and the cost of making those changes. The Software Change Proposal must be forwarded to the Registrar of the Secured Transaction Registry for review and approval before system development is undertaken. Urgent system enhancements must be implemented as soon as possible without need to bundle the correction with other system enhancements. Details of the changes made with regard to urgent system enhancements can be documented after the implementation of the changes.

6. DOCUMENTATION

Documentation must be developed to support the Secured Transaction Registry to facilitate system administration and to inform users of system requirements, functionality and navigation rules. The following is a list of documents that must be developed to support the Secured Transaction Registry.

CLIENT DOCUMENTATION

A. Client Account Agreement

Client agreements must be established between the licensee (as the agent of the Government of Bangladesh) and the clients of the system. This client agreement constitutes a contract between the client and the licensee (as the agent of the Government of Bangladesh). These client account agreements must include:

- A statement of access rights to the database including the use of desktop software if the system is not a true internet browser based system.
- The agreement that users will access the database only through the means, as detailed in the agreement, and that the client will be responsible to pay all government fees for access to the database.
- The statement that the users are responsible for the maintenance and upkeep of their computerized workstations that will be used to access the Registry. The users must also agree that they will use equipment required for the proper use of the system. The user must also accept, under the agreement, the responsibility for all communication costs in accessing the database.
- The warranty that the licensee will take every measure to ensure the continued operation and access to the Secured Transaction Registry with limitations to the hardware and software which remains the responsibility of the client.
- The statements of warranties, indemnities and limitations of liability. These statements include: a confirmation of the rights of the licensee to grant usage rights to the clients, the statement that the licensee will not be responsible for the accuracy of the information submitted by the clients of the system, the statement that government and the licensee will not warrant the operation of the system without interruption and error, however, the government will take responsibility for any faults which may cause a monetary loss to a client (the loss rebated to the client will be no more than the fee associated to the cost of the transaction attempted), the statement that the software provided is on an as is basis (any changes to the software made by the client will be the sole responsibility of the client), the statement that the government and licensee will not take any loss or damages that a third party may claim against a client of the Secured Transaction Registry.
- A statement must also be included in the client agreement that the government has ownership of all of the Secured Transaction Registry related software including the Secured Transaction database software and any client software installed on the client workstations to allow access to the database.

- A statement must also be included restricting the use of the information contained in the Secured Transaction Database. The restriction includes the reengineering of the data to be included in a database accessible to third parties.
- A statement must be included regarding the term and termination rights under the agreement. The term of the agreement shall be on a month to month basis subject to the termination by either party. Upon termination of the agreement, the client will be reimbursed for any unused funds remaining in the client account. The licensee will maintain the right to terminate the agreement at any time should the client contravene any terms of the agreement.
- A statement that the licensee will retain the right to alter the terms and conditions of the agreement at any time, upon having given notice to the client. The client will have the right to immediately terminate the agreement should the changes to the terms and conditions be unacceptable. Use of the system by the client, following receipt of notice of the changes to the terms and conditions, will be deemed as acceptance of the revised terms and conditions. All notices must be in writing.

B. Software License Agreement

Each client who is obtaining a copy of the Secured Transaction Registry desktop software must sign a license agreement. The agreement can be part of the Client Account Agreement or a separate document. The agreement establishes the rights and limitations of user of the desktop software. It contains:

- A statement that outlines the ownership rights of the software and accompanying documentation.
- A statement that the software license agreement gives the client the right to use the client software on any compatible computer for access to the Secured Transaction Registry.
- A statement that the Client cannot: make copies of the software, distribute, rent, sub-license or lease the software, alter, modify or adapt the software and documentation.

- A statement that failure to comply with the agreement will result in immediate termination of the rights to use the software.
- A statement that the software will conform to specifications. Defective software or documentation will be replaced if returned within a required amount of time (i.e. 90 days).
- A statement that the licensee does not guarantee that the software is free of errors.
- A statement that the licensee will not be held liable for any interruption in service.
- A statement that use of the software by the client constitutes agreement to the above terms and conditions.
- A statement that the copy of the software will be obtained for each workstation the client will used to access the Secured Transaction Registry.

C. Software Installation Instructions

To ensure the client software is properly installed on the client's workstation(s), detailed software installation instructions must be included with each copy of the software. These instructions will act as a guide for the users or their technical advisers to properly install the software.

NOTE: To offset the costs of developing the client desktop software, a license fee can be charged to each client for each workstation on which the software is installed. This license fee should be developed not to make a profit but to cover just the cost of development and distribution. See the Business Plan - Section 11 for details.

D. Client Workstation Hardware and Software Requirements

Client must be provided with the minimum hardware and software specifications for the workstations accessing the Secured Transactions Registry. These specifications should outline the type of software to be used, the type of processor, size of RAM required, monitor, graphics, keyboard, mouse, modems and printers. Specifications should also be suggested to ensure maximization of performance.

E. User Guides

User Guides, along with the online Help Text, must be developed for the Secured Transaction Registry. The User Guides will give a description of the purpose of all features available to users, both in the Client Database component and the Secured Transaction Database Component. Further instructions on the use of those features must be included in the User Guides. Use of the menu, menu options and instructions on the navigation rules of the system must be included in the guide. These guides should not be extensive, as on-line help text will be available for each function of the system. To cover the costs of development of the User Guides, clients will be charged for each copy provided.

OPTIONAL CLIENT DOCUMENTATION

F. Batch Uploading of Files Manual

If the batch uploading of files feature is implemented with the Secured Transaction Registry, a manual must be developed specifying, among other things, the format of the files and file limitations.

ADDITIONAL REQUIRED DOCUMENTATION

G. Operations Manual

An Operations Manual must be developed for the Secured Transaction Registry. The Operations Manual will be developed by the software developer for use by the hardware maintenance personnel. This manual will document the configuration of the central databases, associated central database peripherals and the configuration required for client workstations. Trouble shooting processes should be documented in the Operations Manual detailing the causes of errors on the system, what should be investigated should an error occur and corrective actions to be taken. As new enhancements are added to the

Secured Transaction Registry an addendum to the Operations Manual will be developed giving detailed configuration and installation instructions.

H. Maintenance Plan

To ensure the smooth operation of the Secured Transaction Registry, a maintenance plan must be established. This plan will set out what processes will be used for backup, archiving of information, storing and retrieval of search result reports, etc. Some of the regular maintenance processes can be automated while others will require manual processes. A timeframe for performance of the normal maintenance processes will be contained in the agreement and must be agreed to by both licensee and the government.

The processes and procedures contained in the maintenance plan will depend on the decision as to what Secured Transaction Registry software and hardware will be implemented in Bangladesh.

I. Business Continuity Plan

In order to ensure the continued operation of the Secured Transaction Registry a Business Continuity Plan must be established. A Business Continuity plan is a document of steps to be taken should a partial or complete system error occur. The Business Continuity plan will document the degree of urgency and response time associated to any error encountered on the system. Levels of urgency can vary from Level 1 (The highest level of urgency when the entire Registry is not operating) to another lower level when only one client cannot access the system. The plan must include, the action steps to be taken, the contacts to whom varying levels of errors will be reported and the timeframe for continued contact during different levels of urgency. These contacts will include: a representative of the Registrar's Office of the Secured Transaction Registry, a representative of the licensee, a representative of the software developers, a representative of the system maintenance team, a representative of the helpdesk support group.

7. OTHER REQUIREMENTS FOR THE IMPLEMETATION OF THE SECURED TRANSACTION REGISTRY

A. Security

The security of the Secured Transaction Registry is of utmost importance. There is one formula that emphasizes the importance of security in a Secured Transaction Registry. That formula is: **Security + Integrity + Credibility = Sustainability**. Sustainability of the Registry is dependant on the confidence that users have in the integrity of the system Users must be assured that the information accessed is exactly what was entered into the system and that there has not been any tampering with or destruction of the data. Firewalls must be in place to ensure that hackers do not gain access to the database in order to manipulated or destroy data.

Anti-virus software must be installed on the Secured Transaction Registry system to detect the invasion of any viruses, Trojan horses and worms. Norton and McAfee supply virus detection software.

Client accounts must be established. Each user of the Secured Transaction Registry will be issued a User ID and password. The User should be encouraged to change the initial password to one of their choice. The system should require that the password for each User be changed every 30 days. A way of tracking the client must be included in the client setup. The client or the administrative user of a client account must provide some type of traceable ID such as driver's license, tax identification card, etc. associated to the address of the party, when applying for an account. Should something happen so that a client must be contacted the source of ID could be used as a method of tracing that client.

Physical access to the database must also be controlled. People should be able to access the areas in which the servers are housed without first passing security clearance. It is important that foot traffic be controlled in that area.

See Section 9 – Hardware Requirements for Processing Data and Security for further information on security. See also Appendix F – Protection of Computers and the Collateral Registry by Farial Sabrina Anam.

B. Client support. Help desk.

The Helpdesk will deal with questions from clients within their responsibilities. Questions related to the Business Office process should be referred to the Business Office contact. Questions regarding legal issues must be referred to the Registrar of the Secured Transaction Registry. All questions and problems encountered by clients must be logged into a Helpdesk log. The log must contain details of the question and problems encountered. It must also contain details of the assistance given to the clients to resolve of the problems. If problems cannot be corrected at the helpdesk level or if the questions must be referred to a contact within the government or the business office, the contact name to whom the issue was referred must be documented in the log. A copy of the details of the helpdesk log must be sent to the Registrar of the Secured Transaction Registry for review. If the Registrar finds a problem with the advice given or the steps taken to correct the problem, the representative must convey a message documenting the correct response or the correct resolution steps. That message must be in written form.

C. Training.

Public awareness/advertising campaigns should be the first step in training potential users of the Secured Transaction Registry. Representatives of the government and the system administrators should attend meetings of the local law societies, leasing company association, the bankers association and other interested client groups. Without limiting the areas of discussion, the future law, means of accessing the system, system design, hours of operation, fees, requirements to set up a client account, are among the issues to be discussed. The public awareness/advertising campaign will outline the benefits and

use of the Secured Transaction. See Section 11 – The Business Plan regarding the projected costs associated to the advertising campaign.

Client training must be conducted before implementation of the Secured Transaction Registry. As the concept and legislation are new to Bangladesh, sessions must be conducted to outline the purpose and benefits of the new Act, the benefits of use of the Registry and the functionality of the Registry. User seminars should be conducted at the cost of the Government of Bangladesh. These seminars should be a joint effort of the government and the licensee.

Further hands on training should be conducted for clients. To cover the cost of preparing, administering and conducting these hands on sessions each participant should be charged a fee for the training.

Once the system is operational, training should be available to clients at the cost of the client.

Please see Section 11 – Business Plan detailing the costs of advertising campaigns and the training development and delivery.

D. System and Financial Audit

System and Financial Audits must be carried out periodically. These audits should be conducted by an independent agency.

The system audit will review the policies, processes and procedures associated to the operation of the Secured Transaction Registry. A full audit report will be presented to the Registrar of the Secured Transaction Registry detailing the findings of the audit and recommending any necessary changes to streamline the operation of the Registry.

A full financial audit must be carried out annually. The financial audit will review the revenue accounting processes. It will ensure that all revenues are accounted for and that the legislated fees collected have been transferred over to the Government of Bangladesh. The financial audit will review the fee handling policies, processes and procedures associated to the Secured Transaction Registry. A full audit report will be presented to the Registrar of the Secured Transaction Registry detailing the findings and recommending any necessary changes to be made.

8. OPTIONS FOR ACCESSING THE SECURED TRANSACTION REGISTRY

The team discussed the medium by which users will access the Secured Transaction Registry. Two options were presented:

Option 1: Internet access to the Secured Transaction Registry supplemented by Wide Area Network access.

Option 2: Full Internet access to the Secured Transaction Registry.

Option 1: Internet access to the Secured Transaction Registry supplemented by Wide Area Network (WAN) access.

Discussion: It was felt by the team that there may not be local internet access available to all clients of the Secured Transaction Registry. A discussion was held regarding the costs and benefits of using the WAN. There would be no significant software developments costs incurred to set up WAN connection. The hardware costs were much more significant. They are as follow: Additional phone lines would depend on the number of expected registrations per hour/day. Each phone line would cost $500, with a $1000 fixed cost and $200 additional cost per year. Server related hardware devices would amount to: $10,000 for a 32 Port Access Server or $5000 for a Port Master plus the Terminal Server at $5000. These would reside in Dhaka. The additional costs to the clients for use of the WAN could be as high as $.20 per minute from distant districts. No

additional hardware costs would be required of the clients. The benefits are that the WAN is generally more secure and speed is comparatively better through the WAN than the Internet. If the necessary security measures are taken on the Internet connections to the Secured Transaction Registry such as firewalls, encryption methods (VPN or SSL), etc., security should not be an issue.

Conclusion: The additional costs incurred would not significantly benefit the Secured Transaction Registry. This was agreed not to be a viable medium of access.

Option 2: Full Internet access to the Secured Transaction Registry.

Discussion: There would be not additional phone line costs or hardware cost incurred should all clients access the Secured Transaction Registry through the Internet. The clients within close proximity to the Internet Service Provider (ISP) would pay approximate $.01/minutes for connection. The clients from distant districts would incur the same long distance costs as mentioned above in the WAN discussion.

Conclusion: This is the most viable option for all users. They will access the database and the same speed and enjoy the same high level of security.

9. HARDWARE REQUIREMENTS FOR PROCESSING OF DATA AND SECURITY.

It was assumed that the full internet access to the system would be the option chosen in developing the following hardware requirements for the Secured Transaction Registry.

Global technological choices have governed the design of the Secured Transaction Registry. In particular:

- A Web based interface is proposed for its user friendliness and its telecommunication capacity; this kind of interface integrates the newest

functional innovations and has become a standard for distributed operational systems.

- A UNIX platform is chosen.
- An ORACLE database is proposed for its almost limitless capacity of data processing and its many management tools. It is recognized the best data based management system (DBMS) for demanding application needs.

As for the hardware infrastructure proposed, it represents the best solution to minimize initial costs of implementation and it offers the best adaptive solution easily upgradable in terms of processing and storage needs. See Section 11 – Business Plan for a detailed list of hardware components.

- **Centralized management**

A system management infrastructure will allow the electronic monitoring and management of the critical elements (hardware and software) of the Secured Transaction Registry. Technical specialists should get early warning of any anomalies such as hardware failure or threshold overrun, so they will be in a position to take action as soon as possible and avoid critical system failures.

- **Integrated software technology**

The system should be designed to employ an integrated software technology. With respect to the system needs, and the expertise available Microsoft Windows technology should be selected for the Secured Transaction Registry. The Windows 2000 product family would be the preferred choice.

The system design should globally follow the architecture guidelines defined by Microsoft and usually identified by name of DNA (Distributed Network Architecture).

Taking into account the possibility of a major increase in the system workload over time, the need for a high capacity platform may arise. The Data Base Management System should have the possibility to be easily migrated to a variety of platforms. The Oracle DBMS would meet these requirements and therefore should be the one selected for the Secured Transaction Registry.

- **Capacity**

Initially, the system infrastructure should be planned for 350,000 registrations and 110,000 searches per year. Enlistments must stay on the system for at least 6 years unless terminated before then. Lapsed registrations must be retrievable by the enlistment officer for at least 5 years from lapse date. This means that all enlistments must be maintained on the Secured Transaction Database for at least 6 years. After that time the enlistments must be moved over to another storage medium where they remain retrievable by the enlistment officer.

The transaction volumes could increase significantly in the foreseeable future. The systems architecture should be scalable in order to meet needs in a progressive manner by adding new resources and avoiding replacement, if possible.

Requests for registration of transactions originate from the business partners/clients (public network). The distribution between both is unpredictable at this moment.

- **Availability**

Access to the Secured Transaction Registry should be maintained throughout usual business hours, from 7h30 to 21h00, 5 days a week. System interruptions should be planned to occur at night or during the weekend.

Every server should be equipped with redundant disks and power supplies.

Web servers, application servers and DBMS servers should be redundant to ensure a high level of availability. Under normal operation, load–balancing mechanisms should spread the load on all equipment available to maximize response-time.

A. The technological specifications of the Central Registry System

Central Secured Transaction Registry
Other equipment required

i. Application servers

Application servers should be implemented on a Unix platform.

ii. Data Base Management System

The Data Base Management System Oracle 9i Standard Edition should be implemented and operated on a Unix platform and a shared Disk Array. The DBMS should be set up in a fall-over configuration to ensure high availability.

iii. Data archiving on CD-ROM

Electronic registration requests and search reports must be preserved on tape drive files. Tape drives should be installed accordingly.

iv. Firewall

The Secured Transaction Registry should be protected from unauthorized access and from integrity threat by a firewall. The central site should be protected from intrusion and hacking by a firewall.

The firewall should deny any transmission coming from the open network and going elsewhere than the Secured Transaction Registry servers. The Secured Transaction

servers should be the sole equipment visible to the users and the only ones authorized to communicate with the Secured Transaction Registry application servers. Then, the Secured Transaction application servers should be the only equipment capable to communicate with the Secured Transaction Registry DBMS servers where the data resides.

The Cisco PIX 520 should be implemented as the Secured Transaction Registry firewall.

The Cisco PIX 520 should be installed and set up in a fall-over configuration.

v. **Transmission encryption**

The transmission of sensitive date should be protected by encryption. The encryption should ensure confidentiality and integrity of the data during its transmission.

Either Secured Socket Layer (SSL) or Virtual Private Network (VPN) will be used for encryption purposes.

vi. Laser printer

The Secured Transaction Registry will need to produce a number of printed documents such as Notices to Secured Parties. A reliable black-and-white laser printer sustaining a duty cycle of over 100 000 pages per month and a print speed of 24 pages per minute are required. The printer HP LaserJet 8000DN should be installed.

vii. Back-up

A DLT Tape Library should allow for a centralized back-up operation. The library should handle two DLT 35/70 GB units and 16 tape cartridges. The tape library should be connected to the Disk array in fiber-channel aggregated-loop to maximize performance and minimize the Ethernet network usage.

viii. **Mirror imaging of each server – Client Database, Application and Secured Transaction Database.**

All Secured Transaction Registry related servers will be replicated off site on identical servers between 1 and 25 kilometers from the main server location connected through a minimum of 128 kb bandwidth. Presently it is suggested that the mirror servers be connected to the main servers by way of a radio link. Should the option of a high speed Wide Area Network (WAN) link become available before implementation of the Secured Transaction Registry, that option should also be considered.

Figure 2

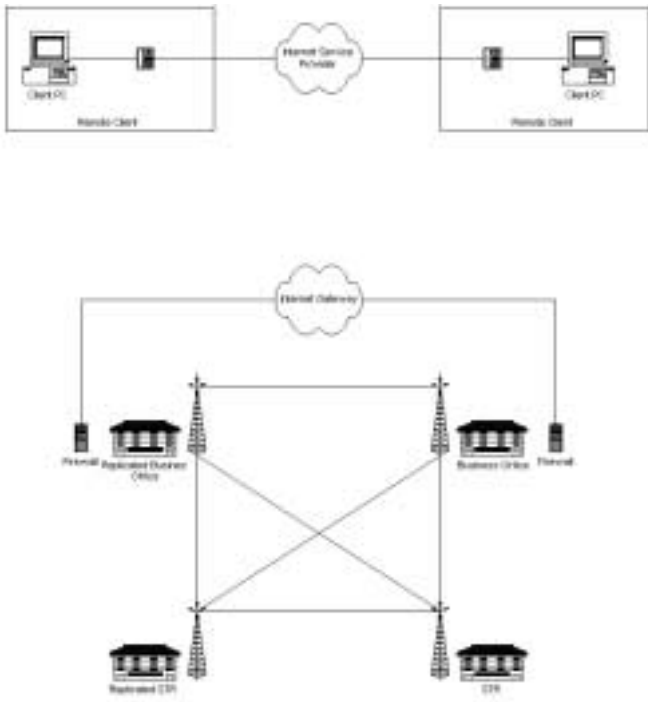


Figure 2 depicts the mirroring of the database. Should the Client Database (shown above as the Business Office) fail, the Redundant Client Database (Business Office) will connect to the Secured Transaction Database. Should the Secured Transaction Database

fail, the Client Database (Business Office) will connect to the Redundant Secured Transaction Database. Should both the Client Database (Business Office) and the Secured Transaction Database fail both the redundant databases will take over. The Redundant databases will be real time copies of the other production databases.

ix. Physical installation

A LAN cabling system should be required. The cabling system should use BDN unshielded twisted pairs with RJ-45 connectors. It shall comply with international standards and shall be certified for 100 Mbits throughput (Category 5 or 6).

The LAN should comply with Ethernet 100Base-T Fast Ethernet specifications. Ethernet switches should be used to dedicate full bandwidth to each server. Ethernet switches should allow for a VLAN configuration to isolate segments.

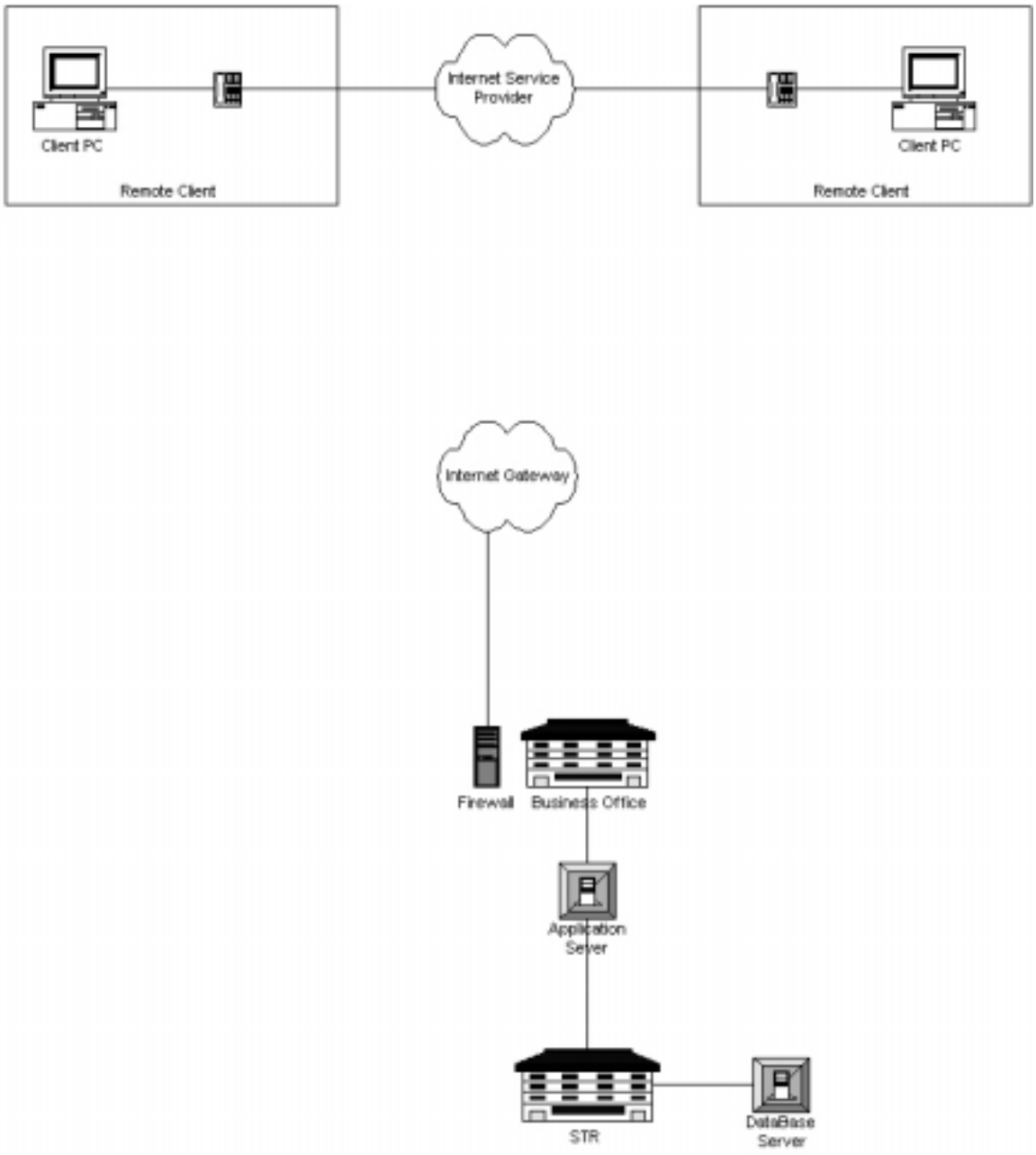
All Secured Transaction Registry equipment should be installed in a 19-inch rack-mounting system.

All equipment should be connected to a voltage stabilizer. Critical equipment should also be connected to an Uninterruptible Power Supply unit.

x. Networking

Public network configuration

Figure 3



xi. Interconnection to public network

The Secured Transaction Registry should be linked to the public network through the Internet to allow connection of business partners/clients.

B. Requirement of the technical environments

Technical environments should be comprised of equipment dedicated to functions other than production. They are usually required for the maintenance and evolution of the system to ensure complete testing proceeding with production.

i. Development and laboratory

A “development and laboratory” environment allows the complete replication of the server configuration of the production environment, aiming at testing any modifications at any level. That environment must be identical to the production and duplicate its complete redundancy.

This is the lone technical environment that fully duplicates the production environment.

ii. Acceptance Test

The “acceptance test” environment aims at final testing before proceeding with production. It consists of simple equipment installed in the secured network areas, in addition to the production equipment.

The “acceptance test” environment is made up of a Business Office server, application server, and a “acceptance test” database instance in the production DBMS.

iii. Training

The “training environment” allows end-users to receive interactive training. Applications are installed on this equipment to be accessible for training purposes only. The environment includes a training database instance that can be altered freely.

The training environment is made of simple Business Office and application server, and a training DBMS server residing as a separate database on the Development Server.

C. Requirements regarding data security and communications

i. Assets to protect

The Secured Transaction Registry is designed as a highly centralized system. Assets to protect are localized at the central site; data, applications and critical systems. These must be strongly secured.

ii. Data stored in the DBMS

The Secured Transaction data is the most sensitive part of the system. Data should be kept, protected and managed by a Data Base Management System.

Data access and data update should be restricted to the only persons explicitly authorized to, with respect to the business rules implemented in the data base system and in the Secured Transaction Registry application.

Based on workload growth expected, the Oracle 9i should be implemented. The Standard Edition is targeted for the Secured Transaction Registry launch, provided that servers targeted are compatible with up to four Intel processors.

D. Requirement for the systems management infrastructure

The Secured Transaction Registry infrastructure should include tools that ensure a constant and complete monitoring of the system's elements.

It should also include the tools required to maintain the software in the business partners/clients public network to plan and achieve successful upgrades.

i. Applications monitoring

The Secured Transaction Registry involves a large number of systems services distributed on multiple servers. Each service has its own parameters and threshold that should be constantly monitored to ensure global system health.

The Secured Transaction Registry should implement monitoring agents for every critical system service: hardware, operating system, Web server, transaction monitor, message queuing, DBMS, proxy servers, directories, load balancing and clustering mechanisms, e-mail, back-up management.

ii. Planned software distribution

To ensure proper management of software in the business partners/clients offices, distribution packets must be prepared and tested. These packets ensure the software installation and should the need occur, the installation rollback. Packets should be launched in a tightly controlled manner, targeting specific workstations and specific timeframes.

E. Hardware and Software Costs for Operating the Secured Transaction Registry

The cost of the hardware and software required to operate the Secured Transaction Registry are outlined in Appendix H. The exchange rate used to calculate the costs was 56 taka/$1US.

10. HOW SHOULD THE SOFTWARE BE OBTAINED?

There are basically two options in obtaining the software. They are:

Option 1: Develop the software in Bangladesh.

Option 2: Purchase a license for software that has been developed for another jurisdiction.

Option 1: Develop the software in Bangladesh.

Discussion: There has been much discussion about the pros and cons of developing the Secured Transaction Registry related software in Bangladesh. One of the advantages of developing the software in Bangladesh is that the software developers would be close at hand. The expertise would be developed in Bangladesh to develop an e-commerce application. Some of the disadvantages of building this system in house are that there is no established expertise in Secured Transaction Registry applications or in developing such a complex application. There also is not a legal expert in Bangladesh who has background in the operation of a Secured Transaction Registry in relation to the legislation. One of the musts in developing the software in relation to the legislation is that the Secured Transaction Registry must be operational and stable to support the legislation. There can be no delays in the system implementation. Also the system must be operating on a stable, error free, environment. A price has been estimated for developing a software package in Bangladesh. Without a full in-depth knowledge of what development entails this estimate may be low. Development of a software package in Bangladesh will take a certain period of time. This presents the risk that the software will not be available when the legislation is proclaimed. It is essential that the software is available the same day that the legislation is proclaimed. There must be a Registry to support the legislation. Software development cost will be an up front cost to the government.

Conclusion: It is for the above reasons that this is the least viable of the options for software development.

Option 2: Purchase a license for software that has been developed for another jurisdiction.

Discussion: There are also advantages and disadvantages to purchasing a developed software package. The disadvantage is that the expertise will not be developed in Bangladesh. That taken into consideration the software providers could train information technology personnel on the maintenance of the software and hardware during the first few years of the operation of the Secured Transaction Registry. A developed software package will probably cost more than that quoted by the software developers in Bangladesh. The advantages are that the software package will have been proven to be stable and error free. The software package would have been developed to work according to associated legislation. Caution should be taken in purchasing an existing package to ensure that the base law for which the software was developed is comparable to the law introduced in Bangladesh. Bangladesh is a Common Law jurisdiction. Software developed to support a Secured Transaction Act in another Common Law jurisdiction would be more compatible with the legislation in Bangladesh that that developed for a Civil Law jurisdiction. The package would include all necessary user documentation. The software would have been proven to work on a specified environment. The software will be ready for implementation in conjunction with the proclamation of the legislation. Cost of the software license can be recovered in a per transaction cost, meaning that the software license fees will be deducted as a certain amount from each transaction fee as transactions are completed on the system. That recovery of the license fees will allow the Government to implement the Secured Transaction Registry without paying the full amount of the software development fees up front. The vendor and all jurisdictions that use the same software can also share costs of enhancements and improvements to the core system functions.

Conclusion: It is for the above reasons that this option is the most viable.

11. Business Plan

The business plan for the electronic collateral registry has been developed for five years including startup activities.

A. Implementation of Services

The services provided through the Secured Transaction Registry system include:

- New registration of an enlistment
- Continuation of an existing enlistment
- Amendment of an existing enlistment
- Termination of an existing enlistment
- Searching services for current and historical records in the system

All the services are envisaged to be provided through clients of the registry system vise a vise, banks, leasing companies, and business lawyers. The clients will set up client accounts with the business office administered by the licensee, set up in the private sector. The licensee is responsible for the administration of the Secured Transaction Registry and provision of the services to different clients. It is suggested that the license given by the Government of Bangladesh to the licensee will be renewable every 5 years. A government office, the Secured Transaction Registry Office within the Government of Bangladesh, is proposed to be set up for regulating the activities of different clients of the system.

The diagram of the organizational chart of the Secured Transaction Registry is shown in Figure 1, Page 17.

B. Technical Feasibility of the System

Considering the Information and Communication Technology (ICT) infrastructure through out the country and the infrastructure groups of potential clients a centralized registry system has been proposed as a core system. For those areas where an ICT infrastructure is not available, service providers who have access to the Secured Transaction Registry will register and search on behalf of infrequent users. Banks, financial institutions and leasing companies may choose to centralize the entry of registrations and searches. Also by doing this the financial institutions will ensure a more consistent entry of data as one person will be responsible for data entry for all branches of the institution.

The technical diagram of the core system is presented in Figure 3, Page 50.

The description of the required hardware specifications including server, network hardware, system software and backup system is presented in the following table.

Table: Hardware and Operating/Database Software Required for the Secured Transaction Registry

Hardware Description	Qty
Router, 1 WAN Connector, 1 dial-up ISDN connector, 2 LAN Ethernet 10/100 connector	**2**
24 Port Ethernet Switch with VLAN Support	**4**
Firewall PIX 520, 6 Fast Ethernet Ports, fall over capacity	**1**
Backup Firewall, PIX 520, 6 Fast Ethernet Ports, fall over capacity	**1**
High Capacity Server, Dual P-III, 4 Processor Capability	
4 Servers with 1024 MB RAM, 2 Hot Swappable 18.2 GB HDD, RAID, Redundant Power, Dual RJ 45 Port	**4**
4 Servers with 1024 MB Ram, 6 Hot Swappable 18.2 GB HDD, RAID, Redundant Power, Dual RJ 45 Port	**4**
35-70 GB DLT Backup Library with Enterprise Backup Management Software	**2**
20-40 GB Internal Tape/DAT Drive	**3**
CD ROM Writer	**3**
P-III PC, 128 MB RAM, 10 GB HDD, RJ45 Port	**10**
Fast Ethernet Cabling	**1**
Basic Rack Mounting	**5**
UPS with Power Conditioning (Online)	**1**
UPS with Power Conditioning (Offline)	**10**
Voltage Stabilizer	**5**
De-Humidifier	**2**
Four Offices Connected by Radio Link (within 25 KM)	

Operating/Database Software	
Operating System (UNIX)	**8**
Data Base (Oracle)	**3**
Anti Virus Software	**10**

C. Management Structure of the System

It is proposed that the government office and business office be established in Dhaka. The client offices, which will interface with the potential secured parties, are planned to spread out through out the country, where required ICT infrastructure is present.

The staffing pattern in the government office Registrar's Office for the Secured Transaction Registry is currently proposed as follows:

- Registrar
- Deputy Registrar
- Receptionist
- Assistant

The registrar is the highest authority of the system. The registrar's office should be established under the direction Ministry of the Government of Bangladesh determined upon entry of the Secured Transactions Act.

The business office will be established in the private sector and will be responsible to the Registrar's Office in Dhaka. The staffing pattern of the business head office is proposed as follows:

- Project Director
- Assistant to Project Director
- Trainer
- Data Base Administrator
- Network Administrator
- Customer Service/Help Desk (2 positions)
- Accountant
- Receptionist
- Security (2 persons x 3 shifts)

The staffing pattern should be changed when the system is converted from the project phase to operation of the Secured Transaction Registry. The actual evolution of the system will dictate the nature of the staffing pattern of the business office. So, it is not prudent to propose any concrete structure of the staffing for the operational phase of the business office.

The growth of the system throughout the country might necessitate increasing the size of the business office in future.

Note: Under the sponsorship of a donor organization an International Consultant could be hired for the first year of operation to oversee the Secured Transaction Registry

D. Logistics and Utilities Requirement for the System

Government Office [Collateral Registrar Office]

Items	Quantity
Car	**1**
Desks	**3**
Chairs	**9**
Meeting Table	**1**
Meeting Room Chairs	**6**
Phone Line Set Up (including phone sets)	**3**
Fax	**1**
Fax Line Set Up	**1**
Air Conditioner	**3**
Interior Decorating	
Internet Access	**1**
UPS	**3**
Photocopier	**1**
Printer (laser jet)	**2**
Gas	
Electricity	
Stationary	

Business Head Office

Items	***Quantity***
Desks	**10**
Chairs	**10**
Desktop PCs & Software	**10**
UPS	**10**
Interior Decorating	
Scanner	**1**
Network Hub	**1**
Phone Lines	**4**
Fax Machine	**1**
Laser Printer	**1**
Air Conditioners	**4**
Stand By Generator	**2**
Internet Gateway	**1**

Mirror Office

Items	**Quantity**
Desk	**1**
Chair	**2**
Air Conditioner	**1**
UPS	**1**
Phone	**1**
Generator	**1**

E. Financial Feasibility of the System

The registry system is proposed to be financially viable. For determination of the financial feasibility initially we have estimate all cost components for the start up period and project period, as well as we have estimate potential revenue to be generated from the system. The estimation of cost and revenue will facilitate to determine the feasibility of the system in the short run and also long run.

F. Costing of the System

The following components have been defined for costing:

1. Government Office (Secured Transaction Registrar's Office)
2. Business Office [including HelpDesk]
3. Hardware Costs
4. Hardware Maintenance
5. Software Procurement
6. Software Maintenance
7. Training Costs
8. Promotional Cost

The details of the cost estimation are given in the Appendix H.

G. Assumptions for Revenue Estimation

(a) Termination of registry is the only service that should be offered free of charge.

(b) Volumes were determined on the basis of 10% of new credit accounts opened each year. Credit account volumes were obtained from Bank of Bangladesh.

(c) Continuations would consist of 2% of the registration volumes.

(d) Searches would consist of 30% of the registration volumes.

(e) Amendments would consist of 10% of the registration volumes.

(f) Generally, term on registration of enlistment is for not less than 5 years. Similarly, a continuation is registered for a 5-year period, but can only be continued in the last year of the registration term. That is why the calculation shown for continuations only appears in the fourth year of the five-year plan.

(g) It is quite understandable that the whole idea of collateral registry for movable properties will take time to get momentum among the potential stakeholders.

(h) Among the potential client groups, initially banks, leasing companies and law firms have been identified.

(i) Is has been estimated that at the end of the project there will 1000 clients of the system.

(j) Expected transaction volumes have been based on information provided by the Bangladesh Bank, and discussions with the banks and leasing companies. The numbers given in the report can only be provided as an estimate. Before implementation of the Secured Transaction Registry a further study of the volume numbers should be reviewed.

(k) In figuring out the fees for the services provided by the system the prime consideration was not to burden the borrowers with additional high costs for obtaining credit. The proposed fees have presented in the following tables.

(l) The first line of the Financial Summary, Source of Revenue shows an amount of revenue from software licenses. That amount is for the desktop software to be provided to clients to install on each their workstations. In calculating that amount it was assumed that there would be 100 copies of the desktop software purchased.

Table: Proposed fee structure for the services

Services	***Fee***
New registration	5
Continuation	5
Amendment	4
Termination	Free
Search [Charge per search]	2

H. Bangladesh Bank New Loan Information

Each registration will be on the basis of opening a new credit account. So, a distribution of the number of accounts among different sectors for the whole financial market will give a precise idea regarding the expected number of registrations for the period of the project implementation.

The numbers shown in the table below indicate an accumulative number of credit counts with the entire banking sector in Bangladesh to December 31, 2000.

#	Sector	Number of loan accounts
1	Agriculture, Fisheries and Forestry	5009924
2	Industry	127602
	Large Scale & Medium	69067
	Small Scale & Cottage	58505
3	Working Capital	71115
	Large & Medium	14967
	Small Scale & Cottage	56148
4	Construction	106381
5	Electricity, Gas, Water & Sanitation Services	357
6	Transportation & Communications	16784
7	Storage	12862
8	Trade	547336
	Wholesale & Retail	510529
	Procurement of Government	3429
	Export Financing	18170
	Import Financing	15208
9	Miscellaneous	1152209
	Total	7041570
	10% increase of total each year	704157

From the above table and from historical data we have found that on an average there is a 10 % increase in number of credit accounts each year. If we consider that all the accounts are under collateral registry against movable assets, the potential number of registry is around 700000. However, it is quite understandable that all the new loans will not fall under this registration process. If we guess that at least 50 % of new credit accounts will be registered under this system, the departure point for revenue calculation will be a with potential volume of 350000 registry, which is quite logical. For the following years we consider a 10% increase in number of registration.

Justifying the projected business volumes in form of registrations of enlistments and searches of the database, the following volumes have been estimated for the projected period:

Moderate Volumes					
Period	Year 1	Year 2	Year 3	Year 4	Year 5
A. Registration	175,000	192,500	211,750	232,925	256,218
Search	55,000	60,500	66,550	73,205	80,526
Continuation	-	-	-	-	9500
Amendment	17500	19250	21175	23292.5	25621.75

For installation of the software at the client's workstation a US$ 100 fee per annum has been proposed. The projection of number of clients and income from license fees is proposed in the following table:

Revenue under Various Scenario
A. Revenue from Software License Fee

	Year 1	***Year 2***	***Year 3***	***Year 4***	***Year 5***
Number of clients	100	400	600	800	1000
Revenue [US$]	10000	40000	60000	80000	100000

I. Costs Associated with Software Procurement form Another Jurisdiction

For off the shelf software procurement] the start up cost has been calculated as sum of fixed costs and one fifth of the operational costs and the following table has been derived form the above calculation:

Financial Summary

Assumption:

1. **Moderate Revenue Projection**
2. **Use of Off the Shelf Licensed Software for Secured Transaction Registry**

Source of revenue	Year 0	*Year 1*	*Year 2*	*Year 3*	*Year 4*	*Year 5*
Registration		875,000	962,500	1,058,750	1,164,625	1,281,088
Continuation						47,500
Search		110,000	121,000	133,100	146,410	161,051
Amendment		70,000	77,000	84,700	93,170	102,487
Total Revenue		***1,045,000***	***1,120,500***	***1,216,550***	***1,324,205***	***1,492,126***
***A.* Operating Expenses**						
Operational Cost for Govt. Office		*29,000*	*31,900*	*35,090*	*38,599*	*42,459*
Salaries(Business Office)		*74,400*	*81,840*	*90,024*	*99,026*	*108,929*
Operational Overhead(Business Office)		*29100*	*32010*	*35211*	*38732*	*42605*
Salaries (Mirror Office)		*6,600*	*7,260*	*7,986*	*8,785*	*9,663*
Operational Overhead (Mirror Office)		*3,800*	*4,180*	*4,598*	*5,058*	*5,564*
Hardware Maintenance		*22,160*	*22160*	*22,160*	*22,160*	*22,160*
Software Maintenance (including enhancements)		*25,000*	*25,000*	*25,000*	*25,000*	*25,000*
Operational Costs for Training		*8,050*	*8,855*	*9,741*	*10,715*	*11,786*
Promotional Cost (Operating Part)		*221625*	*15125*	*0*	*0*	*0*
Operating Costs		*419,735*	*228,330*	*229,810*	*248,074*	*268,166*
Operating Profit		***635,265***	***932,170***	***1,046,741***	***1,156,131***	***1,323,960***
Government Office Setup Cost	***44,475***					
Business Office Setup Cost	***52,400***					
Mirror Office Setup Costs	***12,850***					
Hardware Costs	***302,200***					
Software Costs (US $), OS/Database/Anti Virus	***141,000***					
Secured Registry Software Procurement Cost	***1,000,000***					
Promotional Cost(50% of total Promotional costs)	***236,750***					
Training Cost carried out by Software Developer	***0***					
Startup Training Cost carried out by Government	***7,250***					
Total Capital and Startup Expenditure	***1,796,925***					
Cumulative Net Income	***-1,796,925***	***-1,171,660***	***-249,490***	***757,251***	***1,893,381***	***3,197,341***

Capital requirement (Costs)

For year 0 to 1 of the system operation the cost has been shown as a negative amount as the system development will be an up front cost to have the system developed in Bangladesh.

Software procurement from another jurisdiction could defer the costs over a 5-year period. To defer the costs of software procurement, the vendor would receive a certain percentage of the per transaction revenues received, thus relieving the government of having to cover all costs up front. Details of recovery of the software license fees from another jurisdiction would need to be negotiated with the vendor.

Conclusion:

Based on the costs as detailed in Appendix H, projected volume estimates and the assumptions as detailed in Section G of this business plan it has been determined that the Secured Transaction Registry will realize a return on the investment reached during year 3 of operation. Total cumulative revenue to year 5, using a moderate volume estimate, for example a new registration would cost $5, and a fee structure that will not overburden the consumer, has been estimated at $3,297,341.

APPENDIX A

GLOSSARY

Account – means any right to receive payment for goods sold, pledged, or leased or for services rendered.

Account debtor – means the person who is obligated on an account that has been assigned, or under the terms of a document that has been sold.

Assignment – means the transfer, in whole or in part, of any right in an account, document, title deed, transferable instrument, other intangible property, or any other right to receive payment.

Bankruptcy receiver – means a receiver appointed by a court under the Bankruptcy Act, 1997 (X of 1997) or, if no receiver has been appointed in a bankruptcy case, the court.

Charge – means an *in rem* right to movable property that secures payment of a debt, including the interest held by a pledgee, a hypothecatee, the lessor under a lease as security, the lessor under a lease subject to the Secured Transaction Act, and an assignee.

Charge agreement – means an agreement that creates or provides for a charge, whether or not is called a charge agreement, including an agreement of assignment.

Charged property – means any movable property or fixtures subject to a charge

Client Account – means the individual or company that has been approved to access the Secured Transaction Registry. The relationship between a client account and users under the client account can be one to one, in the case of a sole proprietorship, or many to one, in the case of a financial institution and the credit officers within the financial institution.

Commingled goods – means goods that are physically mixed with other goods in such a manner that their identity is lost in a product or mass.

Debtor – means the person who owes payment of a debt, whether or not the person owns or has rights in the charged property, and includes an assignor, the lessee of goods under a lease subject to the Secured Transaction Act, and a person whose movable property secures an obligation, even if the person does not owe payment of a debt.

Document - means a writing or group of writings that evidences both a monetary obligation and a charge in, or a lease of, specific goods.

Enhancements – means changes to the system as a result of upgrading supporting operating system software, suggestions from clients for increased or improved functionality and the need to correct faults found on the system.

Enlistment office – means the enlistment office established in Section 27 of the Secured Transactions Act.

Field – means a line of entry in the system. For example the line on which an enterprise name is entered would be defined as a field.

Fixtures – means goods that are, or are intended to become, attached to immovable property or fastened to anything attached to immovable property, in a manner that causes a property right to arise in goods under any law relating to immovable property.

Goods – includes all tangible things that are movable at the time the charge attaches, whether or not the are or are intended to become fixtures, but does not include money, title deeds, transferable instruments, or documents.

Helpdesk- means the client support center that will advise clients of the system navigation and functionality.

International Association of Corporation Administrators (IACA)– means a professional association for government administrators of business entity (Joint Stocks) and secured transaction registry systems at the state, provincial and international level in any jurisdiction that has or anticipates development of such systems. IACA works toward the harmonization of legislation among participating jurisdictions related to business entity and secured transaction registry systems.

Judgment creditor –means a creditor who has a right in movable property due to the action of a court.

Lessee in the ordinary course of business – means a person who in good faith and without knowledge that the lease is in violation of the rights of a third party in the goods, leases in ordinary course of business from a person in the business of selling or leasing goods of that kind, either for cash or by exchange of other property, whether secured or unsecured.

Licensee – means an agent of the Government of Bangladesh who is responsible for the administration of the Secured Transaction Registry.

Notice- means a record presented to the enlistment office, and includes records on file or presented for enlistment relating to the initial notice, unless the context indicates otherwise.

Perfect and imperfect rights – means legally recognized rights. Perfect rights are enforceable through court action but imperfect rights are not.

Person – means an individual who has capacity to contract, or any entity recognized by the law of Bangladesh.

Prescribed – means prescribed by rules made under this Act.

Proceeds – means whatever is acquired upon the sale, lease, license, exchange, or other disposal of charge property, whatever is collected on, or distributed on account of, charged property; rights arising out of charged property; to the extent of the value of charged property, claims arising out of the loss or nonconformity of, defects in, or damage to the charged property; and to the extent of the value of charged property and to the extent payable to the debtor or the secured party, insurance payable by reason of the loss or nonconformity of, defects in, or damage to the charged property, and "cash proceeds" means proceeds that are money, checks, funds on deposit in banks, and the like.

Purchase – to take as a buyer, a donee, a person receiving security such as a creditor or mortgagee, or by any other voluntary transaction creating an interest in property.

Purchase money charge – means a charge that is –

i. taken or retained by the seller of goods to secure all or part of its price;
ii. taken by a person other than the seller who, by providing credit or incurring an obligation, gives value to enable the debtor to acquire rights in or the use of goods, if such value is in fact so used.

Record – means information that is inscribed in a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form

Register – means to submit an enlistment, continuation, amendment or termination to the Secured Transaction Database.

Registrant- means an individual who registers an enlistment, continuation, amendment, or termination on the Secured Transaction Database.

Section – means the group of fields of entry associated to one division of entry in the Secured Transaction Registry. A Secured Party name and address is a section of information.

Secured Party – means a creditor, lender, seller or other person in whose favor a charge is created under a charge agreement, including a person to whom accounts or documents have been assigned, and a lessor of goods under a lease subject to the Secured Transactions Act.

Serial Numbered Vehicle – means the following, when held as equipment and not as stock in trade: a motor vehicle, a trailer, an aircraft, or a motorized boat.

Service Provider – means an individual or agency that performs registrations and/or searches on the Secured Transaction Database on behalf of other companies or individuals.

Sign – means to execute or adopt a name or symbol, manually or otherwise, with present intent to identify the signing party or to adopt or establish the authenticity of a record. Sign does not require a manual signature.

Title deed – means a writing evidencing title to goods, or a bill of lading, dock warrant, warehouse receipt or similar record issued by a person in the business of transporting or storing goods.

Transferable instruments – means a record that evidences a right to the payment of money, that is not a charge agreement or lease, which is in ordinary course of business transferred by delivery with any necessary endorsement or assignment, including a check, money order, or certificated security.

UCC Filing application – means the Uniform Commercial Code Filing application in the United States. The Uniform Commercial Code Filing application is the US equivalent of the Secured Transaction Registry in Bangladesh.

User – means an individual under a client account. Each person who accesses the Secured Transaction Registry is a user.

User ID - means a unique identifier code by which an individual under a client account accesses the Secured Transaction Registry.

APPENDIX B
About Check Digits

What is a check digit?

A check digit (CD) is number mathematically derived from the values of digits or characters which constitute identification of a record (e.g., bank account, credit card, etc.).

What purpose does it serve?

While the UCC application is somewhat unique in its use of a CD, the function of the CD is the same in that it involves use of a numbering technique that is designed to automatically trap common presentation errors in numbers such as transposition or substitution errors. Use of a CD will eliminate the reliance on debtor and/or secured party information matching thereby improving the efficiency of both manual and electronic filing.

How is the acceptability of subsequent amendments determined?

Today, filing officers use various subjective methods, such as debtor and secured party name and address matching, to determine that a subsequent amendment to a specific financing statement identified by number is acceptable. Without a check digit, some information matching is required because it is likely that a filer could identify a valid but nonetheless erroneous filing number within the filing office. Use of a CD reduces the likelihood that the filer will identify a valid filing number when the intended number is presented in error.

How will a check digit work in the UCC application?

By use of an automated numbering device, the filing officer assigns a filing number that contains a CD appended to the serial filing number such as 98-123456-7. The CD for this number is 7. If for example the filer erred and identified the number as 98-123465-7 on a subsequent amendment, then the number would be immediately recognized by the filing office as an invalid number thereby requiring rejection of the amendment.

I thought applications that use CD's keep the CD secret, why is it a public part of the number in the UCC application?

In the UCC filing application, the objective is to prevent filing of subsequent amendments to unrelated financing statements where the filer has erroneously identified the filing number. If the filer can present the filing number along with its corresponding CD accurately then it is unlikely that the filer will, unintentionally or without negligence, present an unrelated but valid number.

Does the check digit prevent fraud?

No. The CD in this application is not designed to prevent fraud but rather to prevent the innocent filer errors that occur with some frequency. How is a check digit computed?

There are numerous techniques, but the following outlines the logical steps for a simple single digit and two-digit technique. Realize that these computations are not intended to be completed manually but rather would be contained in a computer program like UCC LabelMaker98 to produce financing statement filing numbers.

Computing the Single Digit Check Number

A typical single digit check number scheme can be up to 90% effective in trapping erroneous filing numbers. The following computations would be executed for a given filing number. Weighting buffer 1,2

Mod 10

Filing number: 98-123456

Step 1 - Assign weights to each digit and multiply each digit by its assigned weight

9 8 1 2 3 4 5 6

1 2 1 2 1 2 1 2

9 16 1 4 3 8 5 12

Step 2 - Total the values derived in step 1

9 + 16 + 1 + 4 + 3 + 8 + 5 + 12 = 58

Step 3 - Divide the sum in step 2 by 10 and use the remainder as the check digit (Visual Basic Mod function returns the remainder, i.e., "58 mod 10")

58 / 10 = 5 with 8 remainder

Check Digit = 8

Step 5 - Append the check digit to the filing number

98-123456-8

Computing Wohler's double-digit Deluxe Check Number

Wohler's routine is effective in trapping 90% of the transposition errors and 100% of all single digit substitution and all multiple digit substitution errors where the difference in the sum of digits is less than or greater than 10. Assuming that say 50% of the filer errors are adjacent single digit transposition and 50% are single digit substitution, then the theoretical error rate would be .05. Assuming that a 50:50 mix of these filing number error types approximates reality, a 95% versus a 90% effective rate may justify the additional check digit.

Weighting buffer 1,2

Mod 10

Filing number: 98-123456

This scheme uses two separate series of steps for computation of each digit of the ultimate check number.

First Digit

Step 1 - Assign weights to each digit and multiply each digit by its assigned weight

9 8 1 2 3 4 5 6

1 2 1 2 1 2 1 2

9 16 1 4 3 8 5 12

Step 2 - Total the values derived in step 1

9 + 16 + 1 + 4 + 3 + 8 + 5 + 12 = 58

Step 3 - Divide the sum in step 2 by 10 and use the remainder as the check digit (Visual Basic Mod function returns the remainder, i.e., "58 mod 10")

58 / 10 = 5 remainder 8

Check Digit = 8

Second Digit

Step 1 - Sum the digits

9 + 8 + 1 + 2 + 3 + 4 + 5 + 6 = 38

Step 2 - Divide the sum in step 1 by 10 and use the remainder as the check digit (Visual Basic Mod function returns the remainder, i.e., "38 mod 10")

38 / 10 = 3 remainder 8

Check Digit = 8

Step 3 - Append the digits to the filing number

98-123456-88

APPENDIX C
Unique Identification Number

How to Uniquely Identify A Person for An Electronic Collateral Registry

By: Faisal Saeed

Introduction

To support the Secured transactions Act it is important to develop an electronic collateral registry where charges on moveable assets will be registered to provide notice to all the potential creditors on charges attached to any moveable asset.

The objective of this paper is to evaluate the best data entry format of the debtor for the collateral registry system. The registry works on a filing system that requires standardization for identification of companies and individuals in order for information to be retrieved efficiently, effectively and accurately.

What is an Electronic Secured Transactions Registry?

An electronic collateral registry is a central enlistment office to perfect (file) a charge on moveable assets. Creditors can retrieve information on whether any prior claim exists on moveable assets and also can file charges on assets in the collateral registry. There are two basic functions of the collateral registry first is to provide information whether any prior claim exists on moveable assets and second is to file charges on moveable assets to set priority in case of a default. The registry plays a critical role in the decision making process of creditors as to whether to provide a loan on a moveable asset.

It is vital to identify the debtor correctly, as only then the registry will serve the purpose of providing prior notice to potential creditors. Designing the retrievial system of data on a particular person in Bangladesh is a complex task as the pattern of names of the population is significantly similar. If a creditor gives a search in electronic collateral registry to find whether there is (are) any prior claim (s) on a machine owned by Mr. Rahim, most likely he will end up with 2000 names stating "Rahim". It is important to identify "Rahim" correctly as only after that the creditor can be sure of what prior claim(s) exists and whether to give the loan.

Design of the data retrieving process

The design of the data retrieving process is (are) field or fields through which a person can be uniquely identified. Fields can be the name, surname, address, date of birth etc. These fields as unique identifiers can be used when the population is being tracked through different tools like birth certificate, voter id card etc. Being a lesser developed country and due to lack of infrastructure and human resource, Bangladesh has failed to use these tools.

So a system has to be developed keeping the following facts in perspective:

The pattern of first name and surname is significantly similar in Bangladesh.
Birth certificates are not mandatory for newborn babies.
Major part of the population is transitional.
Lack of education, which results in lack of interest and awareness among the people.

The fields that can be used to uniquely identify people are:

First Name
Middle Name (optional)
Family Name (surname)
Current address
Permanent Address
Date of Birth and (optional)
Unique Identification Number

The first two fields are the name and family name (surname). In society. a person is usually identified by his name and his family name. Many people can have the same name in Bangladesh. Because of the identical names used these two fields will not uniquely identify a person. The address field can be one solution to this problem but is not recommended as major part of the population has no permanent address. Date of birth can also assist to certain degree, but remembering ones date of birth is uncommon outside of the city. It is not necessary to register the date of birth and the fact that a different calendar year (Bangla Calendar) is followed in the rural areas cause problems with the date of birth being used to assist in uniquely identifying an individual. A unique identification number for individuals would assist in identifying an individual. By searching using a unique identifier number the searcher can ensure that they have found the exact person that they have been looking for. If the criteria does not match with the number, the output of the search result will not result in a name match.

There might be two people with different unique identification numbers with the same first name and surname. The address and date of birth fields narrow down the matches. It is highly unlikely to have two people who share that same unique identification number, first name, surname, address and date of birth.

For a data retrieval process it is important to develop a unique identification number (UIN). To develop a (UIN) for Bangladesh, it is necessary to go through the current tools for identifying people and to analyze them to determine the possibility of selecting one of them as the UIN. The tools that are used to identify the people are:

- Birth Certificate
- Passport
- Driving License
- Voter ID and
- Tax identification Number (TIN)

Birth Certificate (BC): issuance of birth certificate is not mandatory in Bangladesh. The major portion of the population live in the villages. Birth certificate are normally issued only for urban residents as birth certificates are often required for school enrolment. Villages often lack the facilities from which a person can obtain a birth certificate. For those reasons the Birth Certificate will not serve as a method of uniquely identifying a person. Parents are asked to produce birth certificates of their children for immunization, health-care and school enrollment. The Ministry of Local Government[3], suggests using the birth certificate, as an identifier of each newborn Bangladeshi citizen.. Even if it is becomes mandatory to have a birth certificate, it will take another generation for the birth certificate to become useful as an identifier.

Passport Number: Applying for a passport is a costly process, costing as much as Tk. 5000 on average. Usually people request passports only when they are required to cross international borders. Although people from all social levels request passports for international travel, there is not a great number of passport holders. Because of the low number of people possessing passports, passport numbers cannot be suggested as the UIN.

Driving License: It has also been suggested that the driver's license number be used as the UIN. However, like passports, there are not many issued. Driver's licenses are only issued to car owners who represent the upper class. Because of the limited number of driver's licenses issued the driver's license number would not be an effective UIN for individuals.

Voter ID Card (VIC): Bangladesh government started to develop Voter ID card for each eligible voter but the project didn't finish until 2001. The Daily Star, 22 October 1997, reports[4]: "The Voters Identity (ID) Card Project now remains suspended for an indefinite period three years after it was initiated, as the government thinks that 'massive irregularities' took place in the process". The issuance of the VIC is suspended to date. No one in Bangladesh has yet received a VIC. Again because of this the VIC card number cannot be used as an effective UIN.

Tax Identification Number (TIN): The TIN was introduced by the Bangladesh Government as a unique number assigned to every tax-paying citizen in the country. According to the government, every person in the country who has minimum income (Tk. 100,000 per annum) must pay tax and have a TIN. It has bee proposed that a Tax Identification Number (TIN) to be made compulsory for registration or renewal general insurance surveyor, for purchase of land, building sor apartments in areas within the cities and registration or renewal of fitness certificates of noncommercial vehicles..

---

[3] (International seminar on birth registration in city, http://bangladesh-web.com/news/jun/29/nv4n611.htm#A9)

[4] "Voter Identity Card: A Costly and Cursedly Fantasy!", The Daily Star, 25 June, 1998, website: http://www.geocities.com/Athens/Olympus/1186/a250698.htm).

The problem with using the TIN in Bangladesh is that it does not include micro enterprises and micro economic transactions. A person has to pay taxes to the government if they earn more that Tk 100,000 per annum. In an interview in April 1999, Mr. Abdul-Muyeed Chowdhury, Secretary, IRD & Chairman, National Board of Revenue mentioned[5], "There is a total of 677,678 TIN numbers issued in the country". Since 1999, the number of TIN issued has grown steadily.

Why TIN is Unique: To obtain Tax Identification Number, one must fill up a TIN form and submit it. The information required on the form are:

a) Full Name
b) Father's name
c) Name of the Owners (If applicable)
d) Incorporation number (If applicable)
e) Registration Number (If applicable)
f) Current Address
g) Permanent Address
h) Date of birth.
i) Previous GIR (General Index Register) number (if applicable)
j) Signature

A customized computer program generates a TIN. Using the characters in a name it assigns a unique number to a person or an entity. This particular number will be given only to one person/entity and will not be assigned to any other even if the person/entity to which the number was assigned ceases to exist. This will avoid any duplication of numbers.

Is TIN secured enough to act as UIN for the collateral registry? A Tax identification Number puts a person's name in the government list of taxpayers and the state monitors the person on a yearly basis. It's not legal for a person to have two Tax Identification Number's.

A unique Identification Number has to be attached to some sort of state monitoring system, without that, a person can be issued two, three or even more UINs. If the person has more than one UIN he could pledge the same equipment to different financial institutions under different UINs without the financial institution being able to ensure that there are not any previous security interests in the equipment.

Making TIN the UIN for the proposed collateral registry, ensures that it is under state observation. By changing his fathers name, address or date of birth, in order to obtain additional TINs is considered a fraudulent activity which is a criminal offence for which punishable under the laws of Bangladesh.

[5] (The Daily Star, Dhaka, 30 April 1999, website: www.ti-bangladesh.org/olddocs/misc/chowdhury.htm)

The problem of TIN of not including the micro enterprises or person, can also be solved as any person or organization can apply for TIN even when they do not ed to pay taxes because their income is less than Tk 100,000 per year. Having a TIN will solved the problem of filing a charge in the collateral registry of movable goods.

The analysis of different identifiers leads to the conclusion that TIN can be used as the UIN in Bangladesh, as regenerating a whole new system would be costly and therefore not viable.

Conclusion

The design or the fields mentioned above to uniquely identify a potential debtor is optional. Additional research can identify more options or fields that can add value to the system. The data retrieval process mentioned above was designed keeping the limitations in mind such as lack of infrastructure and human resources, a transition population, similar patterns in first names and surnames etc. Before the Electronic Collateral Registry is implemented in Bangladesh, a future review of Uniquely Identifying Individuals should be completed.

APPENDIX D

IACA List of Ending Noise Words

The following words and abbreviations indicate the existence or nature of an enterprise. These business ending will be ignored in a search.

- Agency
- Association
- Assn
- Associates
- Assc
- Assoc
- Attorneys at Law
- Bank
- National Bank
- Business Trust
- Charter
- Chartered
- Company
- Co
- Corporation
- Corp
- Credit Union
- CU
- Federal Savings Bank
- FSB
- General Partnership
- Gen part
- GP
- Incorporated
- Inc
- Limited
- Ltd
- Ltee
- Limited Liability Company
- LC

- LLC
- Limited Liability Partnership
- LLP
- Limited Partnership
- LP
- Medical Doctors Professional Association
- MDPA
- Medical Doctors Professional Corporation
- MDPC
- National Association
- NA
- Partners
- Partnership
- Professional Association
- Prof Assn
- PA
- Professional Corporation
- Prof Corp
- PC
- Professional Limited Liability Company
- Professional Limited Liability Co
- PLLC
- Railroad
- RR
- Real Estate Investment Trust
- REIT
- Registered Limited Liability Partnership
- RLLP
- Savings Association
- SA
- Service Corporation
- SC
- Sole Proprietorship
- SP
- SPA
- Trust
- Trustee
- As Trustee

*__NOTE: The list provided is not definitive. Government representatives and a selected group of system users should make additions and deletions to the above list after review.__

APPENDIX E

Justification of Software Development Costs

Project Manager (Foreign Consultant):

1 year x 200 working days X 8 hrs = 1600 X US$200 = 320,000
Assumed that the time requirements will be 6 months. Cost = 320,000 X 0.5 = 160,000

Legal Consultant:

1 year X 200 working days X 8 hrs = 1600 X US$300 = 480,000
Assumed time requirements will be $1/4^{th}$ of total time. Cost = $480,000 X 0.25 = 120,000

Software Team:

System Analyst -	2 persons
DBA -	2 persons
Project Manager-	1 person
Team Leader -	2 persons
Software Developer -	7 persons
QA -	2 persons
Documentation -	2 persons
Network Analyst -	2 persons
Total	20 persons

Average monthly salary of the total software team will be:
20 X 12 X US$ 500/month = $120,000

APPENDIX F

Protection of Computers and the Collateral Registry System

By: Farial Sabrina Anam

Protection of Computers and the Collateral Registry System

Farial Sabrina Anam
August 2001

Table of Contents

Executive Summary

This report addresses the issues of how to protect the Collateral Registry system against hackers using existing technology (by using usernames and passwords, encryption), ensuring secured access to the server (through the use of firewalls), and protecting data in general (by using anti-virus software, backing up data and ensuring continuous power supply). There are new types of technology that are in the process of being patented and starting to be used more frequently (air gap technology and digital certificates) that could be employed to add a further level of security, especially in the coming years.

Bangladesh should rightly be concerned about the security of the Collateral Registry system that is being developed. There are many security threats existing in the form of viruses, loss of data, hacking and so on. However, despite these threats, if the numerous security mechanisms detailed in this report are employed, they will ensure that the security of the Collateral Registry is preserved and it will function smoothly. The solution is to have layered security, which is the use of many different security measures addressing different aspects, to make it more difficult and expensive for a potential attacker to attempt accessing the system.

Security is a more popular issue now than it was in the past because the Internet has become such a global phenomenon. Because of the way Windows based computers are constructed nowadays, it is easier to hack a computer, or a network of computers, which are connected to the Internet. Modern Windows configurations allows users on a network to share printers and files and unfortunately, a lot of the components are loaded by default once the user has initially logged onto the network, leaving many resources open for hackers. To prevent unauthorized users from accessing internal files on the Collateral Registry, all files should be password protected.

It is anticipated that the Collateral Registry will function in the following manner. The banks that file the information with the Collateral Registry will do so electronically, through the use of Electronic Data Interchange (EDI). This is a system whereby all information passed by a bank to the Collateral Registry will be tracked to ensure that the information received is the same as the information sent, and that it was not altered in any manner.

It is also anticipated that when users want to access the information, they will have to go to the entity that will manage the system and register themselves. This registration will involve filling up paperwork, and eventually receiving a username and password that will identify them uniquely to the server. It is possible that the users will be allowed to access the information remotely (from home or the office) or through terminals in certain government offices (or both). Whatever is the final decision about access, information about all computers that could *potentially* access the system (namely the IP address, otherwise known as the number which uniquely identifies all computers over the Internet) will be known by the Collateral Registry server. This is because the IP address of any computer that accesses another system is automatically downloaded by the system being

accessed. The user is not required to submit any information regarding the IP address as part of the registration process. Thus, attempts to access the system from any unknown IP addresses will be prevented.

One of the simplest methods of security would be to password protect the website. This will ensure that a casual browser will not even be allowed to view the Collateral Registry website, never mind actually trying to do a search on the system.

Encryption of all data on the Collateral Registry system is also advisable. This will ensure that anyone who is trying to access the file illegally will receive a scrambled file, which they will be unable to interpret.

Firewalls are perhaps the most crucial security mechanism that should be used in the Collateral Registry system. Firewalls cannot be said to be a single piece of hardware or software, but in fact are a set of devices that prevent access to a system. The functions of firewalls can be varied, but for the purposes of the Collateral Registry, the firewall will be used to inspect all attempts to access the system from the Internet. Because the firewall can identify a computer by its IP address, it can prevent any computer whose IP address is unidentified from accessing the system.

Up to date anti-virus software must be installed on the Collateral Registry server to prevent worms, Trojan horses or viruses from destroying the hard disk or corrupting files, which would lead to loss of data. McAfee and Symantec are two of the biggest anti-virus software producing companies. It is possible to get anti-virus software which automatically downloads the latest versions on a regular basis (weekly or monthly).

The smooth functioning of the Collateral Registry system can also be addressed by the use of certain measures. Measures to ensure the smooth functioning of the system would be to install a UPS (Uninterruptible Power Supply) so that the frequent power fluctuations do not lead to loss of valuable data (for example when banks are filing their information with the Collateral Registry). It also ensures that users will not face any difficulty when trying to access the information.

Back up options are many and varied. There are numerous back up media available today including floppy disks, magnetic disks, zip disks, read/write CD ROMs and so on. It may be possible to have a dual system so that when data is saved it is automatically saved to two different computers, thus reducing the chances of data loss. It is advisable to back up data every day, if not more frequently. Back up will ensure that if for some reason, data loss occurs, system managers will be able to put the data back in speedily, thus ensuring continuity of service to the users.

It is advisable to use other measures in addition to IP addresses, to prevent access to the server. This is because it is possible to falsify IP addresses. Authentication is this additional layer of security. Authentication can occur in the form of username and password, or what is currently becoming more popular, Digital Certificates. Digital Certificates are analogous to a passport or driver's license and provide irrefutable proof a

person's identity. Although usually used by people to be assured of the legitimacy and safety of a business which has set up its website on the Internet before they buy products from them, in the case of the Collateral Registry, Digital Certificates can be used for client authentication. This means that every registered user can use a Digital Certificate as a login method. Once the Collateral Registry server cross checks the Digital Certificate presented by the user with the issuing authority and ascertains that it is authentic, it can read the fields on the certificate (such as the name of the user) to determine what level of access they should be given to the system. Although Digital Certificates are not widely used yet, they are becoming more popular as time goes by. They can also be thought as being one step better than usernames and passwords, because they can be used as a universal website login, and thus prevents the user from having to remember many passwords. It is also useful for businesses not to have to maintain password databases. In addition, setting up a Digital Certificate with a Certification Authority ensures the use of Secure Sockets Layer (SSL) technology, the standard protocol for secure communication over the Internet. This means that all information that passes between the user's browser and the Collateral Registry server will be encrypted, thus protecting sensitive information like credit card numbers.

A new type of technology that has been developed is known as air gap technology. It should be used in conjunction with firewall technology to provide the maximum amount of protection. While firewalls can provide good protection in terms of preventing initial access to the system from unauthorized users, it can have the vulnerability when users actually try and access information from the databases of the internal network. Air gap technology when combined with firewall technology removes this vulnerability because the external user is prevented from seeing the structure or accessing the internal network. Through the use of a high-speed memory disk, used by both the external network (the Internet) and the internal network, the information requested by the external net users is provided without ever connecting the external and internal networks. Thus, effectively, air gap technology helps provides online access while keeping the external and internal networks physically disconnected.

Thus, concerns regarding the Collateral Registry can be addressed using the above-mentioned precautions. If all these mechanisms are employed, the Collateral Registry should provide a safe, smooth and efficient way for people to access information about collateral that has been pledged by debtors.

INTRODUCTION

The purpose of the electronic Collateral Registry that is being developed in Bangladesh is to allow users to search for information about moveable assets that have been pledged by debtors. Many such registries have been developed and are functioning in Canada, Ukraine, Albania, Croatia, and the United States. This electronic Collateral Registry is a significant component in the Secured Transactions Law, which will provide better access to finance for small and medium enterprises (SMEs). The proper functioning of this electronic Collateral Registry is thus crucial to SMEs receiving credit.

Unfortunately, cyber crime has increased dramatically in recent times, and therefore the security of a Collateral Registry or any electronic data system has to be a priority. The Registry could be compromised in many ways, including illegal access to the system (in the form of hacking) and loss of data (due to viruses, theft, power loss). Hacking is the gain of unauthorized access to a computer system. It can be especially destructive because the owner of the system may not even be aware that access has been gained. Sensitive information like passwords and credit card information can be obtained by the hackers and this can have disastrous consequences. In the case of the Collateral Registry, there is a danger that someone could hack into the database and extract the information without paying the charges, alter the information in the database, or perhaps obtain credit card information of people who have already used the Collateral Registry. To combat these threats, it is possible to utilize existing security mechanisms to protect the main computer that will store the information of the Collateral Registry System.

This report details how to use existing technology to prevent hacking (through the use of usernames, passwords and encryption), ensure secured access to the server (by suing firewalls), and protect data in general (by backing up data, using anti-virus software and ensuring power supply). Additional forms of security could be provided in the form of Digital Certificates and Air Gap technology. If these are employed, the Collateral Registry will provide a safe, smooth and efficient method for users to obtain information about moveable assets that have been pledged by debtors.

SECURITY OF THE COLLATERAL REGISTRY SYSTEM: Protection against hackers, secured access to computers, and protection of data

Why the recent increase in danger to computer systems?

It is important to understand why one has to take more precautions today than in the past. Windows based computer systems are especially vulnerable today because Microsoft added the Internet as an extension of the networking facilities that it had already developed (these networking facilities allowed users to share files and printers). This would be harmless as long as passwords were used. However, it has been seen that on many versions of Windows, passwords are not required once the user has logged in, and in small networks, passwords are often not required at all. In addition, it is possible that even when connection to the network is not required, the components are loaded by default, making the computer more vulnerable to hacking. It has also been observed that Microsoft had optimized the settings for ease of configuration. All of this means that many computers can be accessed over the Internet in the same way a local machine on a

network would be. A single machine (as opposed to one on a network) that is connected to the Internet can also be the victim of hacking.

Different steps can be taken to prevent hacking depending on whether there is a network or Network Interface Card (NIC) attached or not. If there is no network, it is possible to select the option on Windows that prevents users from having access to files while one is connected to the Internet.

However, if there is a local network, this is not a viable option. So, the user has to prevent hacking by using passwords on files. It is advisable to use long passwords (at least eight characters long) because they are much harder to crack than shorter ones. It is also advisable to use alphanumeric passwords (combination of numbers and letters). Common words (such as names of family members or self) should not be used because those are the ones that hackers try first. The judicious selection of passwords is crucial because it is possible to 'guess' passwords. There are softwares called password crackers that are designed to break the security of a system by continuously testing a whole dictionary of passwords until one works. This is called a 'dictionary attack'. There are also programs called password sniffers that can be put on to networks that can capture passwords as they travel through the system. To make the password system stronger, there should be a condition that users will be locked out if they enter the password incorrectly more than three times.

Usernames and Passwords

In the cases of different types of existing Collateral Registries around the world, generally only registered users are allowed to access the services. Someone who wants access to the information has to register themselves with the body which manages the Collateral Registry and obtain a username and password. This means that a person browsing the Collateral Registry website would not be able to have access to the information unless they registered themselves and paid for the information. The Personal Property Registries operating in the provinces of Canada have different rules from each other (because they are managed by different companies), but the general method is the following. Users have to use the Property Registry either in certain Government offices (through public terminals) or remotely (through a personal computer at office or home). In both cases, they have to register themselves with the company that is providing the service. The user does not, however, have to provide information about the IP address of their computer as part of the registration process. This is because any system that is accessed by another computer is able to download the IP address of the computer that is accessing it automatically. This means that no matter how the user accesses the information (remotely or locally), the IP address and other necessary information of all computers that could *potentially* access the system will be known. Thus a firewall can prevent access from any unknown terminal. Any unknown user will be viewed as a potential attacker.

A further level of security in the form of a username and password for the website itself could be employed. This would prevent a casual browser from even viewing the site. After the registered user enters the appropriate username and password, they will be

allowed to view the site, and access information in the database by using other usernames and passwords.

Encryption

Another option would be to have all sensitive information encrypted using Massachusetts Institute of Technology's PGP (Pretty Good Privacy) or a similar product. Encryption is a system of using a mathematical equation to change characters into something else so that no one other than the intended recipient is able to read the message. Although used primarily to encrypt emails, PGP can also be used to encrypt files, disk volumes and network connections. Encryption cannot help against theft or deletion of information, however.

In the case of the Collateral Registry system, encryption could perhaps be used so that a user who is trying to access the information by means of hacking will receive an encrypted file. The only way to read the information in an unscrambled form would be to access the information in the normal manner and paying for it.

Firewalls

Firewalls are also recommended as a security precaution in the case that cables or DSL modems are being used (which implies that a computer is constantly connected to the Internet). This is what will occur in the case of the Collateral Registry.

A firewall is not really a single piece of hardware or software. It is more a system of network security devices. It may be a combination of devices that protect one network from others. Firewall configurations should be made to fit the requirements of the network in question. The network manager should be concerned about possible access from the Internet and through the internal network. Firewalls should be installed between every possible source of intrusion and the information that is being protected. In the case of the Collateral Registry, the most applicable one is obviously access to the network through the Internet.

The purpose of a firewall is to identify and prevent access from machines over the Internet. To understand how firewalls work it is important to understand how information is transferred over the Internet. Information is broken down into 'packets' of data, which may take different routes to their destination. Once received, the recipient sends an acknowledgement to the source. In order for two computers to communicate in this manner, each 'packet' contains the address of the originating machine (made up of the IP address and a port). Ports are created by software to permit certain networking functions. For example, Web access is usually Port 80. In order for hacking to occur, the perpetrator must gain access to an open port in the machine. A firewall examines each packet of information before any other software on the computer accesses it. Hence the firewall can completely control the receipt of anything from the Internet.

A firewall can have varied functions. It can be used to filter out packets based on any combination of the originating computer's IP address and port and that of the destination computer's, or to allow outgoing connections while preventing any incoming connections to be made. Firewalls can also be a method of logging and auditing for the network

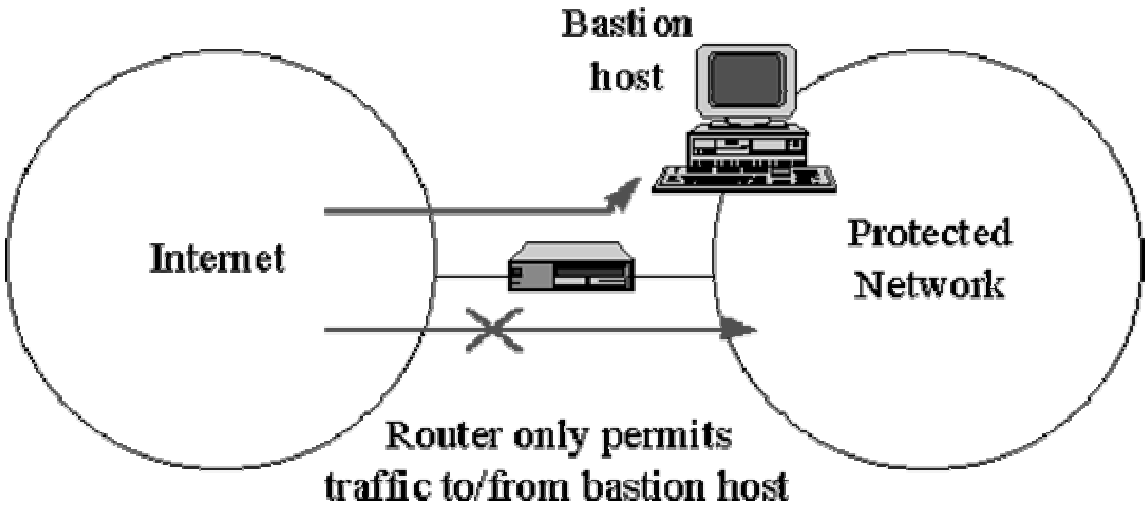
administrator because it shows the quantity and type of traffic that flows through the network, how many attempts were made to break it, and so on. Firewalls can be used to block access to certain sites on the Internet and also to prevent users on one server from gaining access to another in the same organization. In the case of the Collateral Registry, the most important function of the firewall would be to prevent unauthorized users from gaining access to the information on the database, and to the system itself.

There are generally two types of firewalls: network layer and application layer. The distinction between them is that network layer firewalls make their decisions depending on the source, destination addresses and ports in individual IP packets. On the other hand, application layer firewalls do elaborate logging of traffic passing through them, in addition to some other functions. It appears, therefore, that for the purposes of the Collateral Registry, a network layer type of firewall will be the most applicable.

The most basic of firewalls is made up of a router that is used as a choke point. This means that all packets passing to and from the network are stopped at the choke point and inspected.

A more complex type of firewall would include chokes as well as gates and packet filtering. The gate is often a computer on the network which behaves as the mail server and the Internet access point (also known as bastion hosts). Filtering (also called screening) is to allow the router to group packets based on where they originated and where they are going. Filtering will stop packets from any unauthorized addresses.

Screened Host Firewall:



The above diagram is of network layer firewall called a Screened host firewall. In a screened host firewall, access to and from a single host is controlled by means of a router operating at a network layer. This single host is known as the bastion host.

Router

Limitations to firewalls include: attacks that do not come from the firewall (example, theft of the computer itself), viruses, or any other 'data driven attacks' (when something is mailed or copied onto a machine inside the network where it is then executed).

It has been mentioned that the firewall will prevent access based on the IP address of the computer that is attempting to gain access. One issue of concern is the fact that it is possible to falsify one's IP address. It is because of this that some sort of authentication is usually required. Authentication can take the form of a username and password. Most of the Personal Property registries in Canada use this method. Some have more stringent rules than others - for example, in Nova Scotia, any user who is trying to access the terminal locally is assigned a user ID on a daily basis that is destroyed after the user pays for the services. Digital certification is another form of authentication.

Data Driven Attacks - Viruses, Trojan Horses, Worms

It is best to start off with some definitions, as many people are not aware of the differences between viruses, Trojan horses, and worms. A virus is a replicating code segment that attaches itself to a program or data file. Viruses may or may not contain attack programs or trapdoors. On the other hand, a Trojan Horse is a software entity that appears to do something normal but which, in fact, contains a trapdoor or attack program. A worm is an independent program that, when run, copies itself from one host to another and then runs itself on each newly infected host.

The way to prevent viruses, Trojan horses and worms is to have up to date anti-virus software (freely downloadable from the Internet) that is run every time the system is rebooted. This will ensure that such programs originating in floppy disks and the Internet are destroyed. The major anti-virus software companies keep their software up to date. Some packages are designed to download updated versions of the anti-virus software on a regular basis. It would be prudent to do the same with the computer which will store the information for the Collateral Registry to ensure that data about moveable assets that have been pledged by debtors is not wiped out because of a data driven attack.

Although emails and attachments are probably not applicable to the discussion to the topic of Collateral Registry, it is useful to know that there are anti-virus software packages that scan downloaded files and incoming emails and attachments automatically. McAfee and Symantec (Norton) all produce such packages.

Power Supply

In a place like Bangladesh, where continuous power supply is not guaranteed, it is a necessity to invest in a UPS (Uninterruptible Power supply) so that voltage fluctuations do not result in loss of data or damage to the hard disk. The UPS also ensures that the user, in the event of power loss, will continue to receive information from the database.

Back ups

It is important to keep back ups of all data on other media in case the hard disk crashes, or a virus corrupts files. Nowadays there are many options available, like floppy disks, zip disks, magnetic tapes, read/write CD ROMs. If something like a hard disk crash does

occur, it will be possible to reinstall the information into a new hard disk from the back up sources.

Other possibilities include the use of dual systems, which means that when data is saved, it is done to two different systems simultaneously. The chances of both systems losing data are unlikely, and so provides an extra level of security. In addition, the second system could be stored in a separate physical location to increase the security. There should daily incremental back ups (to store all information that was filed that day) to whatever back up media is chosen, and weekly system back ups of all the information on the Collateral Registry to the back up media. The back up media could also be stored in a separate physical location.

Security while filing Moveable Assets

Banks will presumably do most of the filing of moveable assets. In that case, a method such as the one existing in the United States can be employed. There, the filing (known as Uniform Commercial Code (UCC) Filing) is done through EDI (Electronic Data Interchange). Security for the EDI in America was achieved by the use of "value added networks" (VANs). The purpose of a VAN is to provide security and connection between networks. The way it does this is by tracking the information that is filed and ensuring that the data received by the filing office (in this case, the entity which will manage the Collateral Registry) is the same as the one sent by the filer (in this case the bank concerned).

While paper filing of moveable assets in the United States could take anywhere from days to weeks, the EDI filing system cuts the process down to two minutes. The EDI filing system was first adopted in Texas. A similar kind of process could be adopted for the Collateral Registry in Bangladesh.

Digital Certificates

Nowadays the cost of creation of websites is very low and it is also easy to copy existing webpages. By using these tactics, con artists can produce webpages and pass them off as being those of a genuine organization's. They do this in an attempt to obtain sensitive data like credit card information from unsuspecting customers.

Users who will be submitting their credit card information over the Internet to get information from the Collateral Registry will want to know that their sensitive data will be protected and that they are in fact accessing the correct website.

This is where Digital Certificates can play a role. Digital certificates can be likened to a passport or driver's license which give irrefutable proof of a person's identity. VeriSign and GlobalSign are one of the biggest issuers of these types of Digital Certificates (also known as a Server IDs). Such organizations are known as Certification Authorities (CA). A Certification Authority does thorough research into the organization that is requesting the Server ID to make sure that the organization is what it is really claiming to be. Once satisfied of the legitimacy of the company, they will issue a Server ID. The presence of a Server ID assures the user that they are accessing a legitimate website.

In the case of VeriSign, the Server IDs work with Secure Sockets Layer (SSL) technology. This is the standard protocol for secure communication over the web. Once the VeriSign Server ID is installed onto the business's server, SSL is automatically activated, which allows secure communication to begin between the business's server and the customer's browser. SSL fulfils the following functions: it allows the customer to verify that the website belongs to the company and not to an imposter, and it encrypts all information which is transmitted. When a message is sent, the sending and receiving computers create a code based on the content of the message. If even one character is altered, the code will reflect it. Users going to sites which have been secured in this manner will know of it by the presence of a 'padlock' icon in the browser window, or by the fact that the URL is 'https' and not 'http'.

Just as Digital Certification can be used by the customer to ensure the authenticity of the company, it is possible to have client authentication on the part of the business. It would be prudent to have this kind of mechanism in the Collateral Registry. The Collateral Registry could use client digital certification to ensure that only authorized users are accessing the information.

The way a client digital ID would work in the case of the Collateral Registry (at least with VeriSign's) is the following: when a user visits the website, the server will request a digital ID from the user's browser. The user will select the ID (if they have more than one - or they could choose to have a default ID) that they want presented to the server. The Collateral Registry server will then verify the ID presented. Once the ID passes the check, the Collateral Registry server will read the different fields of the digital ID which will tell it who the user is, and will then allow the user to access appropriate resources in the site. All of this takes about 1 second to complete.

Digital Certificates could be said to be one step better than usernames and passwords. This is because while it is possible for a third party to intercept passwords which are passing through the Internet (if some from of encryption is not used), there is no such danger with Digital Certificates. It will also be more convenient for the user in that they will not have to remember numerous passwords. It will also save expenses for the business in terms of not having to maintain and support password databases. The digital IDs can serve as a login for any website on the Internet which accepts digital IDs.

Users can obtain digital IDs by going to the websites of VeriSign and GlobalSign and filling up the necessary forms.

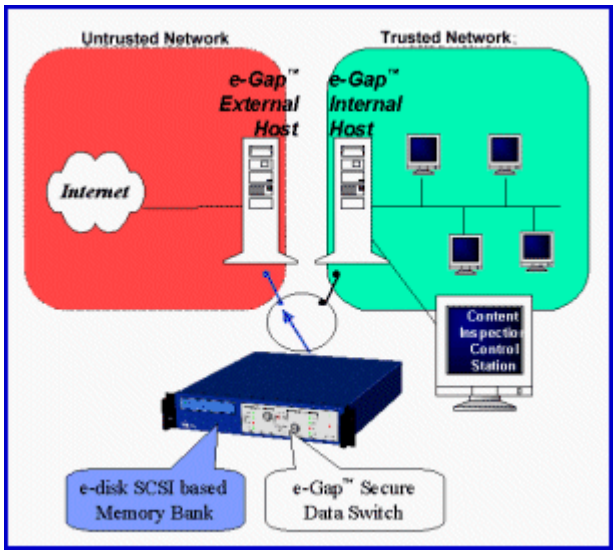
Air gap technology

Air gap technology is a theory that has been applied to create the e-Gap System by Whale Communications. It has not been patented yet, but shows promise, especially in the realm of real time applications as is common with e-commerce. A so-called 'air-gap' is maintained between the untrusted Internet, and the trusted internal network. Through the use of Air gap technology, online data transfer between these two entities is allowed while keeping them physically disconnected. The way in which this occurs is the following: There is an autonomous, non-programmable switching device (called the Small Computer System Interface (SCSI) Based Memory Bank) which serves as the

memory for two hosts which are connected to the external and internal network. The memory bank is a high-speed e-disk that alternates between the two computers, but is never really shared by or connected to both the hosts at the same time.

The e-Gap helps make e-business secure because it allows access by unknown users to internal data in a safe manner - the e-Gap system does not allow any TCP/IP packets to enter the 'back office'. The way the e-Gap system works is by preventing the potential hacker from seeing the internal structure of network. This means that they cannot see the authentication server or the username database. All that the potential hacker would be able to see is the external computer which is connected to the SCSI device, and as such, they have no way of knowing what is on the internal network.

A diagram is provided for reference:



Source: "Whale Communications - FAQ" http://www.whalecommunications.com/030001.htm

Essentially, Air Gap technology helps to give real time access to the Internet without exposing the risks of the firewall. Firewalls have a vulnerability in that to give external net users access the databases of the 'back offices' (or the Internal network) a hole must be opened from the De-Militarized Zone (where the firewall resides) to the back office. This 'hole' allows only a certain type of traffic in and out of the back office. But if a hacker can pass off as being part of this traffic, then they can gain access to the back office. Air gap technology takes care of this problem by allowing access to the back office without opening such holes in the Firewall. Thus the vulnerability of the firewall can be removed by using it in conjunction with air gap technology.

According to Whale Communications, the types of industry that are most likely to benefit from a system such as e-Gap are real time business applications like on-line banking, business to business secure file and email transfer and supply chain integration, to name a few. Medium to large enterprises such as financial institutions, telecommunications operators, on-line retailers, and similar institutions will also benefit. Air Gap technology will be applicable in the case of the Collateral Registry - which essentially involves the purchase of a service (information) over the Internet.

This system is useful for e-commerce because the separation between the e-commerce web servers and the internal corporate databases can be kept intact. Security sensitive industries like Government, Military, Defense and so on can also use Air gap technology. These organizations are often so concerned about cyber terrorism that they even go to the extent of physically disconnecting internal networks, thus leading to 'network islands' which are separated from other internal (or external) networks. The introduction of air gap technology would allow these organizations to maintain the type of security they enjoy when they are offline, while permitting the transfer of information between networks.

CONCLUSION

Layered security is the practice of using many different security mechanisms to protect a network. It is far more prudent and more powerful to use anti-virus software, firewalls and air gap systems together to build a barrier than to use any one of these systems by themselves. Layered security makes it all the more difficult and expensive for potential attackers to enter the system, making it less likely that they attempt to do so and more likely that they are unsuccessful if they do.

A very basic level of protection can also be that the website could be password protected. There could also be a condition such that any user who enters the wrong password more than three times would be blocked from accessing the services. The use of anti-virus software, back up systems and UPSs is crucial, and go without saying. Firewalls can programmed to allow requests to access the system only by users who have registered themselves with the company which will manage the Collateral Registry in the proper manner. It will make use of the IP addresses of all computers which could potentially access the system to offer protection in this manner. However, since there is the possibility of changing IP addresses, authentication will have to be carried out to verify that the person accessing the system from a certain computer is really the person who has been authorized to do so - and this is where usernames and passwords or Digital Certificates play a role. In order to reduce the vulnerabilities of the firewall, air gap technology should also be used in conjunction with firewall technology to allow access to the databases in the internal network in a safe manner.

Given the use of these many security mechanisms, the online Collateral Registry can be safe from current forms of malicious attacks. However, a close watch should be kept on all developments in the security industry, and when appropriate, should be applied to the Collateral Registry system in Bangladesh.

Definitions

The following definitions were taken from "Internet Firewalls: Frequently Asked Questions" and "Security Portal - Glossary - Security 101"

Access - Entrance granted to a specific user such that they have the ability to get the information they want or need.

Administrator - In technical terms, someone who manages security and user access, usually for larger computer systems, such as universities and corporations, but technically on any scale.

Authenticate - To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Authorization - The process of granting or denying access rights to network, resources, programs, or processes.

Cryptography - The science concerning the principles, means, and methods for rendering plain text unintelligible, and for converting encrypted messages into intelligible form.

Data Driven Attack - A form of attack that is carried out by maliciously encoding a seemingly innocuous piece of data, which is executed by a user or a process to unknowingly cause damage. A data driven attack is a concern for firewalls, since it may get through the firewall in data form and launch an attack against the system behind the firewall.

E-Commerce - The exchange of goods and services between business and consumers/other businesses over the medium of the Internet.

Encryption - A change made to data, code, or a file so it no longer can be read or accessed without processing or decrypting.

Firewall - A system or combination of systems that enforces a boundary between two or more networks, or a gateway that limits access between networks in accordance with local security policy.

Hacker - A person who enjoys exploring the details of computers and how to stretch their capabilities. Often construed to mean a malicious or inquisitive meddler who tries to discover information by poking around.

Hacking - Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network.

Hard Disk - A magnetic disk that can store computer data. Hard disks hold more data and are faster than floppy disks.

Host - A single computer or workstation, connected to a network. Often refers to a computer which hosts services.

Internet - A communications network consisting of countless networks and computers around the world.

IP - Internet Protocol - the protocol by which data is sent from one computer to another on the Internet.

IP address - A unique number address used to identify a machine on the Internet. (ie. 123.456.789.012). IP addresses conform to the IP.

Network - Two or more machines connected for the purpose of data transfer. Networks allow users to have access to data on different drives, servers, and other networks.

NIC - Network Interface Card - the hardware card that serves as an interface between a network and a computer.

Packet - A block of data sent over the network transmitting the identities of the sending and receiving stations, error - control information, and content.

Password - A series of characters, usually without spaces, that is unique to a single username. A password is leveraged to determine the authenticity of a user.

Port - As a network term, port refers to a specific position in device memory that is remotely accessible, and through which network data is routed.

Protocol - Agreed upon methods of communications used by computers. A specification that describes the rules and procedures that products should follow to perform activities on a network, such as transmitting data. If they use the same protocols, products from different vendors should be able to communicate on the same network.

Remote access - The ability to get access to a computer or a network from a remote distance. Dial-up, dedicated lines, ISDN, wireless, cable modem and DSL technologies all permit remote access.

Router - An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer. A router acts like a traffic cop standing in an intersection -- it routes information to where it needs to go. Some routers are more intelligent that others. A good router can even make detours on the fly. Routers are often the targets of DoS attacks.

Server - Any computer or software program that serves another computer or software program (the client). A server usually provides network services such as disk storage and file transfer.

SCSI - This is one type of standard interface used to connect PC components, such as CD-ROM drives and Hard Drives.

TCP/IP - Transmission Control Protocol/Internet Protocol - These protocols in tandem govern how computers communicate over the Internet . The TCP controls how and when the IP sends and receives packets.

Trojan Horse - A software entity that appears to do something normal but which, in fact, contains a trapdoor or attack program.

Virus - A replicating code segment that attaches itself to a program or data file. Viruses might or might not contain attack programs or trapdoors.

Worm - A standalone program that, when run, copies itself from one host to another and then runs itself on each newly infected host.

Works Cited

"PGP Freeware", http://web.mit.edu/network/pgp.html

"Internet Security - Protection against Hackers",
http://www.corinna1.freeserve.co.uk/esecurity.htm

"Internet Firewalls: Frequently Asked Questions", http://www.interhack.net/pubs/fwfaq/

"Firewalls and security for Computer Networks",
http://home.att.net/~gobruen/progs/networking/firewalls.htm

"Internet Security at a Glance",
http://www.securityportal.com/research/security101/internetsaag.html

"Safe Internet: Microsoft Privacy and Security Fundamentals",
http://www.microsoft.com/privacy/safeinternet/sniffer/default.htm

"Frequently Asked Questions, Air Gap Technology for e-Business and Air Gap Technologies", http://www.whalecommunications.com/0300.htm,
http://www.whalecommunications.com/,
http://www.whalecommunications.com/030001.htm

"Nova Scotia Personal Property Registry",
http://www.acol.ca/Services/PPR/NS/access.html

http://www.isc-online.ca/isc_public/scripts/isc.asp?cfgpage=SIGNIN

"An Overview of a Canadian Personal Property Security System ",
http://www.natlaw.com/pubs/overview.htm

"Guide to Securing your Web site for Business",
http://www.verisign.com/rsc/gd/srv/secure-bus/secure_web-site_guide.html

"Accepting consumer Digital IDs at your Web site - FAQ",
http://www.verisign.com/clientauth/faq.html

"Enabling your web site to accept consumer digital IDs",
http://www.verisign.com/clientauth/

"Securing the Perimeter, Part 2",
http://enterprisesecurity.symantec.com/article.cfm?articleid=783

"The Importance of Layered Security", http://
enterprisesecurity.symantec.com/article.cfm?articleid=767

"Remote access and remote access server (RAS)",
http://iroi.seu.edu.cn/books/whatis/remoteas.htm

"Electronic UCC Filing Faster and Cheaper",
http://www.govtech.net/magazine/gt/1995/jun/features/secstate.phtml

"CFA Standards at Work: EDI Streamlines UCC Filings in Texas",
www.cch-lis.com/update/ucc_filing_guides/cfa_efiling.html

APPENDIX G

Marketing

To popularize the concept of collateral registry for movable assets and encourage financial institutions, lawyers and other possible stakeholders a set of marketing tools should be selected. The marketing should target the following groups:

1. Potential entrepreneurs who will go for bidding to be the Licensee of the whole system
2. Financial institutions including banks, leasing companies, who are potential clients of the systems
3. Lawyers who will facilitate the borrowers and other stakeholders to get the services of the system along the legal support.
4. Borrowers who do not have access to credit due to the lack of immovable property holding.
5. The government and Bangladesh, who play a facilitating and regulating role to ensure security, prevent fraud and building confidence among the stakeholders.

For segmentation of the market and selecting an appropriate marketing mix, a survey should be conducted.

Initially, it is quite understandable that huge promotional campaign is required to sensitize, create public opinion in favor of enacting a secured transaction law, which will create enabling environment for the financial institutions to enhance access to credit by the SME borrowers. A huge promotional plan has been proposed to achieve the objective of the project. While selecting the media for the promotion newspaper has been emphasized initially. However, other media vise a vise. Radio, TV, internet are also important. To create awareness among the policy makers, lawmakers, government executives, financial institutions, seminars, workshops and roundtable discussions have

been proposed in the promotion plan. The whole campaign has been planned for the first two years and also before formal launching of the project. The costing of the promotional campaign has been presented in the financial feasibility section.

Item	Year 1	Year 2
Awareness Campaign for Stakeholders through Seminar, Workshop, Roundtable	49000	-
Advertisement in Newspaper	72000	-
Advertisement in Radio	20000	-
Advertisement in Electronic Media [TV, Internet]	136000	-
Development and Dissemination of Promotional Materials	30250	30250
Total	307252	30250

Awareness Campaign

Event	Frequency	Cost	Total Cost
Seminar	4	3000	12000
Workshop	10	2500	25000
Roundtable	4	3000	12000
			49000

Advertisement in Newspaper

Type of paper	Frequency	Cost per advertisement	Total Cost
Bangla Daily[4]	200	200	40000
English Daily [2]	70	200	14000
Specialized Magazine	60	300	18000
			72000

Campaign in Electronic Media

Type of program	Frequency	Cost	Total Cost
Special Program	4	10000	40000
Sponsorship	10	4000	40000
Advertisement	140 x30 second ad.	400	56000
			136000

Development and Dissemination of Promotional Materials

Type	Quantity	Frequency	Cost	Total Cost
Poster	50000	2	0.3	30000
Brochure	500000	2	0.2	20000
Booklet	2000	3	1.75	10500
				60500

APPENDIX H

Cost Projections

COST PROJECTIONS

Operating Costs: Government Office

	Year 1	Year 2	Year 3	Year 4	year 5
Logistics and Utilities					
Internet Access	500	550	605	666	732
Telephone	6,000	6,600	7,260	7,986	8,785
Fax Line Charges	2,400	2,640	2,904	3,194	3,514
Gas/Driver	6,000	6,600	7,260	7,986	8,785
Electricity	900	990	1,089	1,198	1,318
Stationary	1,800	1,980	2,178	2,396	2,635
Total Logistics and Utilities Costs	***17,600***	***19,360***	***21,296***	***23,426***	***25,768***
Salaries + Other Benefits					
Registrar	4800	5,280	5,808	6,389	7,028
Deputy Registrar	4200	4,620	5,082	5,590	6,149
Receptionist	1500	1,650	1,815	1,997	2,196
Assistant	900	990	1,089	1,198	1,318
Total Salaries for Government Office	***11,400***	***12,540***	***13,794***	***15,173***	***16,691***
Total Operational Costs for Govt. Office	**29,000**	**31,900**	**35,090**	**38,599**	**42,459**

Operating Costs: Business Office

Salaries (Business Office)	Year 1	Year 2	Year 3	Year 4	year 5
Project Director (1 position)	24,000	26,400	29,040	31,944	35,138
Assistant to Project Director	6,000	6,600	7,260	7,986	8,785
Trainer	6,000	6,600	7,260	7,986	8,785
Data Base Administrator	12,000	13,200	14,520	15,972	17,569
Network Administrator	12,000	13,200	14,520	15,972	17,569
Customer Service/Help Desk (2 positions)	6,000	6,600	7,260	7,986	8,785
Accountant	3,000	3,300	3,630	3,993	4,392
Receptionist	1,800	1,980	2,178	2,396	2,635
Security (2 persons x 3 shifts)	3,600	3,960	4,356	4,792	5,271
Total Salaries (Business Office)	***74,400***	***81,840***	***90,024***	***99,026***	***108,929***
Business Office Operational Overhead					
Office Rental	11000	12,100	13,310	14,641	16,105
Internet	3600	3,960	4,356	4,792	5,271
Phone Bill	11000	12,100	13,310	14,641	16,105
Stationary	3500	3,850	4,235	4,659	5,124
Total Operational Overhead (Business Office)	***29100***	***32,010***	***35,211***	***38,732***	***42,605***

B. Operating Costs: Mirror Office

Salaries (Mirror Office)	Year 1	Year 2	Year 3	Year 4	year 5
Maintenance (1 person)	3,000	3,300	3,630	3,993	4,392
Security (2 persons x 3 shifts)	3,600	3,960	4,356	4,792	5,271
Salaries (Mirror Office)	**6,600**	**7,260**	**7,986**	**8,785**	**9,663**
Mirror Office Overhead					
Office Rental	3000	3,300	3,630	3,993	4,392
Phone Bill	500	550	605	666	732
Stationary	300	330	363	399	439
Total Operational Overhead (Mirror Office)	***3800***	***4,180***	***4,598***	***5,058***	***5,564***

C. Hardware and Software Maintenance Cost

	Year 1	Year 2	Year 3	Year 4	year 5
B. Hardware	**22160**	**22160**	**22160**	**22160**	**22160**
Software (including enhancements)					
Case A (for locally developed software):	**52325**	**52325**	**52325**	**52325**	**52325**
Case B (for off the shelf procured Software)	**(25000)**	**(25000)**	**(25000)**	**(25000)**	**(25000)**

Training Cost

D. On going Training carried out by business office

Monthly training for 40 people at Dhaka office(US$ 10 x 40 person x 12 month = US$4800 annually)	4800	5,280	5,808	6,389	7,028
5 training in divisional head quarters per year each session having 20 people(US$ 10 x 20 x 5 = US$1000)	1000	1,100	1,210	1,331	1,464
Travel Expense of the Trainer (1 Trainer)For five divisional head quarters	1,500	1,650	1,815	1,997	2,196
Accommodation Cost of the Trainer for each training and also for the each divisional head quarter	750	825	908	998	1,098
Total Operational Costs for Training	**8,050**	**8,855**	**9,741**	**10,715**	**11,786**

Promotional Cost

Item	Year 1	Year 2	Year 3	Year 4	year 5
Awareness Campaign for Stakeholders through Seminar, Workshop, Roundtable	24500	0	0	0	0
Advertisement in Newspaper	36000	0	0	0	0
Advertisement in Radio	10000	0	0	0	0
Advertisement in Electronic Media [TV, Internet]	136000	0	0	0	0
Development and Dissemination of Promotional Materials	15125	15125	0	0	0
Total Promotional Cost (Operating Part)	***221625***	***15125***	***0***	***0***	***0***

Note: Total promotional cost has been divided into two components: 50% has been considered as operating costs and 50% as start up costs

Capital and Startup Expenditure

(including Software Development Cost)

Government Office Setup Costs

Car	25,000
3 Desks	300
9 Chairs	675
Meeting Table	250
6 Meeting Room Chairs	450
Phone Set Up Costs	2400
Fax	450
Fax Line Set Up Cost	800
Air Conditioner	8100
Interior Decorating	750
Internet Access	500
3 UPS	300
Photocopier	2500
Printer	2000
Total Government Office Setup Cost	***44,475***

Business Office [including Helpdesk & Mirror Office]

10 Desks	900

10 Chairs	850
Desktop PCs & Software	9800
UPS	1000
Interior Decorating	4000
Scanner	500
Network Hub	400
Phone Lines (including call distribution)	2500
Fax Machine	450
Laser Printer	1000
4 Air Conditioners	11000
Stand By Generator	18000
Internet Gateway (high speed connection)	2000
Business Office Setup Cost	**52400**
Mirror Office (Fixed Costs)	
Desk	100
2 Chairs	150
Air Conditioner	2700
UPS	100
Phone	800
Generator	9000
Mirror Office Setup Costs	***12850***
Total Business and Mirror Office Setup Costs	**65250**

Start up Promotional Cost

(50% of total Promotional costs)	***236,750***

Training Cost carried out by Software Developer (relevant only software is developed locally)

Production/Design of Training Manual	5,000
Training Material (For 300 people, 5 session in Dhaka & 10 at divisional head quarters)	2,500
Travel Expense of the Trainer (2 Trainers)	3,000
Accommodation Cost of the Trainer	1,500
Training Site Accommodation	5,000
Startup Training Cost carried out by Software Developer	***17,000***

Startup Training Cost carried out by Government

Organizational Cost					5,000
Travel Expense of the Trainer (1 Trainer)					1,500
Accommodation Cost of the Trainer					750
Startup Training Cost carried out by Government					**7,250**

Hardware costs for Setting Up STR

Description	Qty	Unit Price (USD)	Total (USD)
Router, 1 WAN Connector, 1 dial-up ISDN connector, 2 LAN Ethernet 10/100 connector	**2**	**6598.95**	**13157.89**
24 Port Ethernet Switch with VLAN Support	**4**	**2631.58**	**10526.32**
Firewall PIX 520, 6 Fast Ethernet Ports, fall over capacity	**1**	**5263.16**	**5263.16**
Backup Firewall, PIX 520, 6 Fast Ethernet Ports, fall over capacity	**1**	**5263.16**	**5263.16**
High Capacity Server, Dual P-III, 4 Processor Capability			
4 Servers with 1024 MB RAM, 2 Hot Swappable 18.2 GB HDD, RAID, Redundant Power, Dual RJ 45 Port	**4**	**12280.7**	**49122.81**
4 Servers with 1024 MB Ram, 6 Hot Swappable 18.2 GB HDD, RAID, Redundant Power, Dual RJ 45 Port	**4**	**15350.7**	**61402.81**
35-70 GB DLT Backup Library with Enterprise Backup Management Software	**2**	**7017.54**	**14035.08**
20-40 GB Internal Tape/DAT Drive	**3**	**1400**	**4200**
CD ROM Writer	**3**	**438.6**	**1315**
P-III PC, 128 MB RAM, 10 GB HDD, RJ45 Port	**10**	**1140.35**	**11403.51**
Fast Ethernet Cabling	**1**	**8771.93**	**8771**
Basic Rack Mounting	**5**	**5263.16**	**26315.79**
UPS with Power Conditioning (Online)	**1**	**10526.32**	**10526.1**
UPS with Power Conditioning (Offline)	**10**	**192.98**	**1929.82**
Voltage Stabilizer	**5**	**350**	**1750**
De-Humidifier	**2**	**3508.77**	**7017.54**
Four Servers Connected by Radio Link (within 25 KM)			**70,200.00**
Total Hardware Costs(US $)			**302,200**

Operating/Database/Anti Virus Software Procurement [Fixed Costs]

Description	Qty	Unit Price (USD)	Total (USD)
Operating System (UNIX)	8	10000	80,000.00
Data Base (Oracle)	3	20000	60,000.00
Anti Virus Software	10	100	1000
Total Software Costs (US $)			*141,000.00*

Secured Registry Software Procurement Costs:

Under the assumption the Secured Registry Software can be procured off the shelf and the cost is estimated to be US$ 1,000,000 (which will include initial training and maintenance cost for five years).