Strategic Planning for Informatics

Canadian Passport Office

Final Report

February 19, 1992

David Clark
Wade Frembd

David A. Clark & Associates Inc.

Strategic Planning for Informatics

Canadian Passport Office

Final Report

February 19, 1992

David Clark
Wade Frembd

David A. Clark & Associates Inc.

Strategic Planning for Informatics

Canadian Passport Office

Final Report

February 19, 1992

David Clark
Wade Frembd

David A. Clark & Associates Inc.

Table of Contents

1. Introduction and Summary.

In the late summer of 1991, the Passport Office of the Department of External Affairs and International Trade Canada was contemplating an internal review of its computer systems and its uses of informatics technology. Although the computer systems in place were supporting day-to-day operations in an efficient manner, they were nearing their capacity limits as well as approaching the end of their life cycle. The PPO also recognized possible new growth paths that existing computer systems were not able to provide.

As a result, the Passport Office ("PPO") decided to initiate a process of long range strategic planning for informatics over the next decade. The objective of this exercise was primarily to provide the PPO with a proper high level view to guide its specification and implementation of new systems and technologies in the short and medium term.

The first step in this process was the initiation of an independent consultant's study, incorporating a review of current computer operations, difficulties or limitations being encountered, and emerging technologies that might affect the PPO. The result of the study was to include a draft of a high-level plan that would permit the PPO to complete its detailed planning process in the context of the study results.

The study took place in the latter part of 1991, and this document represents the final report of study results and recommendations.

Conclusions.

The PPO issues more than 1.2 million passports per year, plus other travel documents, and the demand for this service has been increasing at an average of 6.5% per year for several years. These processes are accomodated very efficiently in the PPO, which rightfully prides itself on high levels of service provided at reasonable cost to the public. Services are available at a number of locations in Canada and at EAITC missions abroad, although there is limited or no on-line access

to HQ computer files from remote offices. Canada has also been a leader in working with the International Civil Aviation Organization (ICAO) and international colleagues in the design and development of counterfeit-protected machine readable passports.

During the study, however, it was realized that to appreciate fully what the future direction of informatics should be for the PPO, it was essential to examine the global and technological trends that would influence and perhaps alter the focus of the PPO during the same period. This is so because informatics is in fact of fundamental significance to the PPO; the primary mandate of the PPO now and particularly in the future can realistically only be realized with the computer technologies available. In other words, what the PPO hopes to achieve in terms of services is driven or constrained by what informatics technology can provide. Informatics awareness must therefore be considered as both strategic and tactical in nature.

The media exposure in the fall of 1991, which occured as the study was underway, underscored this point of view. The apparent evidence of easily obtained fraudulent passports resulted in the recent announcement of a number of operational changes, including more direct personal contact by applicants with PPO offices and reduced availability of mail order passport services. Yet such a change, while necessary, would ideally also involve an on-line linkage for application processing between the many issuing offices and the HQ computer files. Assessment of the security objectives of the PPO results in the conclusion that on-line computer links to all issuing stations is a necessary condition to future informatics plans.

The study therefore did consider not only emerging 90's technologies that might influence the PPO but also social and political concerns of the next decade that may be expected to "pull" the PPO into new service directions and which will also enable the PPO to augment its role in a proactive manner. Some of the concerns reviewed were:

- Societal pressures - there will likely be increased volumes and security demands for passports and other travel documents, highlighting the activities, data integrity, and methodologies of the Passport Office.

- Enabling technologies - will provide many practical means for passport security enhancements, both intrinsically and extrinsically. This is very significant since these technologies are also available to counterfeiters.

- Political pressures - Criminal counterfeiting as well as the growing need to identify fraudulent passports and their carriers upon presentation can be expected to create international pressure for new security developments in passport technology. Increased Immigration focus at borders, including Canada's, can be expected to result in the prospect of controlled data access to the PPO data base files for authentication.

- Management awareness - of enabling technologies through common experience in everyday life with developments in personal computing, networks, client-server applications, and in credit card/banking systems, will create an expectation for improvements and new measures for passport security and service. The PPO should be in a position to provide proposals to government managers for better security, on-line authentication, and modernized distributed facilities rather than react after the fact.

- Strategic integration - of PPO roles, systems and networks, and data resources into overall government strategic plans and operational programs can also be expected as a result of the above. This integration, which need not be organizational but rather operational in nature, will become a stronger motivation as the PPO modernizes its application systems into the 90's, and as government leaders are made aware of the potential benefits arising from these changes.

Recommendations.

1. As a result of the study, it is recommended that the PPO examine and embark on an early program to restructure its operations to create an on-line processing environment to link all of its offices and other issuing locations, as well as permit later connection of other potential users such as Immigration, for passport validation purposes.

2. In specifying new computer application systems, the PPO should incorporate emerging technologies for digitization of images such as photographs and signatures, and also develop corresponding document image work flow and management operational systems. These technologies, already being installed in several Canadian government organizations, will become a dominant technological force in the 90's.

It is difficult to imagine a more appropriate technology for the PPO than image capture and management, since it offers, among other attributes:

- o Greatly enhanced security, through the on-line accessability of file photos and signatures, and perhaps fingerprints, that can be reproduced on a computer screen at a border point to match to the equivalent information and images on the passport itself;

- o Integrated application data capture and storage of all relevant and multi-media elements of the application (photographs, signatures, application data).

- o Document flow processing, for the fully automated control of passport work flow. Rather than circulate the paper documents to all stations, the process can be automated and made paperless, with the entire file - including data, photo, and signature as well as a readable image of the original application itself - "appearing" at the workstation of each of the control points in sequence during the approval and issuance process. These kinds of systems find their best advantage in large volume applications such as the PPO.

- o Additional service opportunities. The use of on-line multi-media data bases will permit the PPO to offer a variety of additional services regarding the authentication of passports and passport data. This possibility can greatly enhance the real contribution of the PPO to mainstream government policies and programmes, and also permit the expansion of its role to

include the provision of special services to other governments and even to the private sector.

3. It is also recommended that the PPO take steps to alter the passport and its production to permit digitized information, including photographs and signatures, to appear directly on the passport itself. Although all of the same technologies would still be available to counterfeiters to prepare a false passport, as is the case at present, the easy on-line access to computer verification of such items, along with increased focus by Canada on validation at its borders, can serve as an effective deterrent.

4. It is recommended that the PPO refine the high level implementation plan and timetable presented as "Strategy A" in this report, in order to develop a detailed fast track to the implementation of revised computer procedures and security over the next 4-5 years.

5. It is recommended that the PPO begin collecting basic "biometric" data, including at least photos and signatures as well as basic personal and ID data, as soon as possible in a form that can ultimately be transferred to or used directly by the eventual new system. The reason for this recommendation is that the PPO requires a full 5 years to renew all passports issued, and it would be highly advantageous to have the data base ready when the cut-over to the new system is achieved.

An implementation scenario to correspond to the above recommendations was developed for this report, and demonstrates how a universal imaging and work flow management system can be achieved and made available in all PPO offices and in foreign missions. The capital costs for equipment for such a program over a 4-5 year period is suggested as approximately $3M. The detailed calculations behind this figure are, however, based on current technology costs which are sure to decrease significantly over the next few years of the PPO implementation period.

2. The Present Passport Office

In order to address appropriate future directions for the Passport Office (PPO), it is necessary to present some details on the history and traditional roles of the organization, along with a description of its current "profile" or operating characteristics as perceived by the study team. These serve as a useful tool in explaining the strategic directions discussed and the evolutionary path for planning the changes recommended.

2.1 History

The issuance of passports to Canadian citizens has been a service of the Government of Canada since its inception, and followed in the tradition of the British practice in this area after Confederation. Originally possessed almost as an honour, their use was limited only to those more senior or wealthy individuals who travelled internationally. For many years no pictures or other identification were included, and the mere possession of the passport documentation was sufficient to prove citizenship and identification.

This mode of operation underwent many changes in the twentieth century, due to a number of factors such as wars and the displacement of large numbers of people, and the ready availablilty of travel, particularly air travel, by most individuals. The passport remained as a fundamental means of identity, but became much more commonly used and requested.

Inevitably the advantages of fraudulent possession and use became apparent to many. In 1968, James Earle Ray, the assassin of Martin Luther King, was found to have 3 falsified Canadian passports in his possession at the time of his arrest. This and other concerns led to the formation of the MacKenzie Royal Commission, whose recommendations resulted in the relocation of the Canadian passport function into the Department of External Affairs, and the establishment of the present security function and a distribution of offices across the country. Other recommendations of the Commision for increased security, such as the use of fingerprints and use of RCMP for issuance of passports in remote locations were rejected by cabinet at the time.

Since this reorganization, the Passport Office has operated quite independently from External Affairs, financed solely by the fees it collects. In recognition of its specialized and user-funded orientation, it has recently been made a Special Operating Agency of the federal government, although still technically part of External Affairs and International Trade Canada (EAITC).

The demand for passports has continued to grow over the years. The first automation equipment was installed in approximately 1976 as an aid in producing an ever increasing number of passports. The current computer system was installed 5 years ago to upgrade production facilities, and has been expanded as required since then to meet ever increasing demand for service, which since 1986 has averaged 6.5% annually. Actual counts of passports during this period is as follows:

Passports issued: Year	Count	Increase
1986/87	981,000	
1987/88	1,061,000	8.1%
1988/89	1,100,000	3.6%
1989/90	1,195,000	8.6%
1990/91	1,269,000	6.2%

In addition to its primary mandate, the PPO has formed cooperative links with a number of counterpart organizations in other countries, such as the State Department in the USA, the UK Passport Agency, and the Australian Department of Foreign Affairs and Trade. Immigration officials from many of these countries are also involved in such cooperative efforts, including Employment and Immigration Canada. Although different countries define and use their own passport and border entry requirements, they have also worked together under the initiatives of the International Standards Association (ISO) and the International Civil Aviation Organization (ICAO) in the development of common standards for passport size and formats. ICAO, with regard to its UN air travel support role, is currently spearheading international efforts in this regard, and the Canadian PPO has been an active participant in the ICAO program to define Machine Readable Passports (MRP's). The PPO itself converted to production of MRPs in 1985.

The primary thrust of these passport developments has been to increase the security

of passport possession and use, and to prevent fraud. Despite the many security features now built in to passports in accordance with ICAO standards and special safeguards used by each country, there nevertheless have been serious concerns again raised recently regarding the growth of the illicit trade in fraudulent passport applications and possession[1]. These developments can be expected to increase focus on the passport and Passport Office operations, subjects that will be dealt with further in this report.

2.2 Primary Products and Services

The primary function of the Passport Office involves the issuance of a number of official travel documents, including regular (blue) passports, special (green) and diplomatic (red) passports, Certificates of Identity and Refugee Travel Documents.

Passports are issued to Canadian citizens who can demonstrate that they meet the qualifications by submitting applications at any of a number of offices within Canada or at missions abroad. The current application system is based very much on the principle of self recognizance to avoid fraudulent application, since although guarantors are required along with "official records" of birth certificates, etc, it is not possible presently to verify each application with the original source reference.

Applications for passports may be made by mail or in person both in the National Capital Region (NCR) or at various regional Offices. The main NCR office is in Hull, Quebec, while regional offices are located in Vancouver, Toronto, and Montreal with local offices at approximately 23 locations across Canada. These regional and local offices provide a walk-in service for applicants. Applications received via mail or from the House of Commons are processed in the NCR.

The Passport Office has successfully concentrated on processing the majority of walk-in applications within 5 working days, and mailed-in applications within 14 days. External Affairs provides a passport replacement service through the facilities

---

[1] pg 1, *The Gazette*, September 18, 1991

of their foreign missions, to service expatriate Canadians and those travellers who may have lost their passports while abroad.

2.3 Document Statistics

The count of passports issued in each region for fiscal 1990/91 is as follows:

	Count	% of Total
Eastern	286,000	22.5%
Ontario	352,000	27.7%
Western	272,000	21.4%
NCR	287,000	22.6%
Foreign ops	71,960	5.7%

Diplomatic and special passports are issued to diplomats and government officials as required, and must be returned to the Passport Office at the end of the mission. These are only issued by the Ottawa office. 1,633 diplomatic passports and 8,463 special passports were issued by the Ottawa office in 1990/91.

Certificates of Identity (C of I) are issued as travel documents for residents of Canada who are unable to obtain passports from their country of origin but who are not refugees. Approximately 3,000 C of I documents were issued last year.

Refugee Travel Documents (RTD's) are issued as identity and rights documents for legal refugees admitted into Canada. Approximately 3,000 RTDs were issued last year.

Certificates of Identity and Refugee Travel Documents are only issued from the HQ office in the National Capital Region.

3. Mandate and Objectives

The official mandate of the Passport Office is legally defined by the Canadian Passport Order of June 24, 1981. Under this order, the Passport Office is to issue, revoke, and/or withhold passports to Canadian citizens. The act also defines the basic type of evidence required to accompany an application.

As a Special Operating Agency, the Passport Office must break-even financially over 4 year financial periods. A maximum $4 million gain or loss in any one 4 year period is permitted. Fees charged are usually changed only every 4 yrs, and this fixed-fee period is 2 years out of synchronization with the financial period in order to permit adjustments in fees to ensure break-even operation within the financial period. Any accumulated surpluses in any 4-year financial period are carried forward.

3.1 Objectives

With this operational and financial mandate, the Passport Office has evolved as an efficient service organization. In fact the PPO lists as its primary objectives the following key elements:

1. Service to "customers"
    - o Fast response times on applications
    - o Quality control of passports and other documents
    - o Integrity and reliability of passports, to enhance world wide acceptance

2. Cost control

   - o Cost per passport and productivity measurements
   - o Achievement of financial mandate - balanced books

3. Security Practices

   - o Counterfeiting detection and control
   - o Appropriate scrutiny of applicants
   - o Information from and to Immigration, Canadian Police, etc.

4. A Responsible Employee Environment

   - o Continuing review and improvement

5. Product Improvement

   - o Look and content of passport
   - o Integrity and reliability of passport

The above objectives are often contrasting and must be balanced. For example, rapid service comes at a higher staff and operating cost, particularly given the increases in volume reported above. Also, increased security checking of passport applications cxauses both delays in processing time as well as increased costs. This latter truth is something that the PPO must come to address in view of the security concerns recently raised.

All of these objectives are very much the present operating concern of the PPO, and are measured where possible on a regular basis. Application turnaround times and productivity costs are charted, and the PPO have traditionally initiated a number of improvements to production techniques, validation procedures, and quality

assurance steps. Its service orientation is very much in evidence, and the character of the operation is one of efficiency, awareness of customer needs, and a quality product.

3.2 Strategic Evaluation for the Future.

In addressing the strategic directions appropriate to the Passport Office in its use of computer technology, it was necessary to consider the overall history and current objectives and profile of the PPO, since so much of its fundamental operation revolves around the computer system facilities. An evaluation of objectives is essential to determine where weaknesses exist; for example, increases in demand might result in untenable cost increases due to the incapacity of the computer system to accomodate growth. Similarly, a wider distribution of Passport office locations will complicate the computer system operation and increase the demand for larger networks. An increased focus on security concerns, for example the validation of guarantors or more detailed verification of application documentation, will also have a large potential impact on future computerization directions.

These legitimate influences exist within the present mandate and focus of the PPO. It was also necessary, however, to consider other influences, ones that may well arise out of expected or possible developments in society and technology in the 90's. These factors will exert their own influence on the operation of the PPO, either directly or as a result of social and/or political pressure. Some of these developments have the potential to alter and increase the focus and strategic relevance of the PPO in overall government programs.

The following are the main areas of consideration for strategic evaluation:

- Business and social trends in the 90's.
- Possible government policy shifts
- The nature and impact of emerging technologies

- Increased need for special passport security
- The strategic relevance of passport data bases

These will be examined in greater depth in the next sections with focus on their possible impact on the Passport Office. Despite the inability to predict the exact nature of these influences, it became apparent during the study how the nature of these factors, taken together with the present operational focus and issues of the PPO, permitted a useful framework for strategic information technology planning to be developed and proposed.

4. Business and Social Trends of the 90's

In 1981 any predictions made of the events to unfold in the next 10 years would doubtless have been wrong. This 10 year period was a time of great upheaval, including the democratization of many eastern block countries, the end of the cold war and the elimination of the Communist party in the USSR, the tearing down of the Berlin Wall and re-unification of Germany, the Gulf War, and changing world positions towards Iran and Iraq.

The last decade saw, too, the growth and technical sophistication of international terrorism, including bombings and the kidnapping of Western hostages. The criminal element also became increasingly sophisticated in the smuggling of cocaine and other illicit drugs, associated also with elaborate international money laundering schemes.

Many of these developments were facilitated by the use of stolen or forged passports, including Canadian ones, and a significant impact on the PPO can be expected with increased focus on these issues. Of primary concern here, however, is to realize that the 90's are also unpredictable, and one can be certain that many suprises and upheavals can be expected. It is only possible here to attempt to look at areas where some reasonable predictions can be made and to try to understand the potential impact of these types of influencs on the Passport Office.

4.1 Increased Travel for Trade and Tourism.

One clear trend in the world today is the rapid evolution of large trading blocks and free-trade zones, such as the European Common Market, North America (Canada, USA, and Mexico), and possibly the Pacific Rim as well as the new free market Eastern Block. Members of these trading blocks trade with each other and with other blocks, usually under the growing influence of GATT rules. In addition, many large corporations are becoming "internationalized", with plants and offices in strategic locations around the world to minimize manufacturing costs and be close to key markets.

These developments will be possible because of the opening of trade barriers in free trade zones and the general growth in global trade. Unforseen factors which may considerably enhance these trends include the possible opening up of China after their 1997 takeover of Hong Kong, and the potential effect of renewed economic growth of former members of the USSR.

Another factor to consider is the continuing growth of tourism, particularly tourist travel to more widespread "exotic" locations around the world, such as Thailand, India, or Africa. Improvement to aircraft costs and flying speeds and distances can be expected to continue to continue during the 90's, particularly considering how the Canadian (and Western) demographic profile will change; the population will increasingly be comprised of older individuals with more leisure time and money for travel.

As business and tourism becomes more globalized, more Canadians will have need to travel to foreign countries. Present growth in passports issued averages 6.5% per year - this is significantly faster than the population growth rate of approximately 1% per year for the same period [2], and appears to be fuelled even now by both business and personal travel. Although fluctuations can be expected with economic cycles, there is no reason to believe that growth in passports issued will not continue at least at the current rate or even expand further for the foreseeable future.

4.2 Increased Focus on International Travel Security.

With increased travel by people from all countries and growing problems with illegal immigrants around the world, the need for Canadians to rely on their passport as a credible and accepted travel document will become increasingly important. Should incidents of international terrorism and crime continue or rise, there will be increased demand for fraudulent Canadian passports and increased scrutiny of passport holders by immigration officials. In fact, the impact of drug trafficing around the world may result in an agreement among many countries to impose new standards on minimum travel document requirements and verification safeguards for international travellers.

---

[2] Calculated from *Quarterly Demographic Statistics*, January - March 1991, Statistics Canada

The incentives for such increased security include the need to control the flow of immigration and refugees from impoverished Eastern-Block countries, from countries such as Haiti and Vietnam, and from wealthier countries such as Hong Kong. Australia already requires a visa for all visitors, which must be provided to Australian or airline officials before travel commences; checks are carried out during the travel itself to certify that entry for this individual,is acceptable.

4.3 Availability of technology for counterfeiting purposes.

The technology used now or projected for use in producing passports is also already available to criminal elements. The sophistication of passport forgeries is expected to at least keep pace with passport technology, and may, in fact, lead it if international crack-downs on illegal identification is implemented and travel documentation requirements become more stringent. Criminal elements or terrorists can adapt to new techniques faster than a government.

As a result of this process, many countries may come to realize that the only absolutely reliable means to confirm authenticity of a passport or to verify identity of the holder will be by electronic query to the passport issuing authority. Such a query will of necessity require confirmation that such a passport is issued and not reported lost or stolen, and that the holder and passport is the same as the picture on file. Similarly the issuance process itself will have to be made as secure as possible in order to minimize the risk that a genuine passport is not issued in fraudulent circumstances. All of these possible developments, aided by enabling technologies and their use by undesirable elements, will have a profound effect on passport issuing organizations around the world.

This subject will be discussed further in section 6 below.

5. Government policy shifts

The 90's will almost certainly see many changes to government policy, whether within the present party rule or as a result of the election of other political parties to power. Many of these policy shifts will occur as a result of international and social changes rather than specific party platforms, and will directly affect the PPO. For example, as a result of current immigration trends, the Canadian government is already acting to reach agreements with the governments of the United States and Mexico to control the flow of refugee claimants into Canada. [3]

Immigration Focus at Borders.

The locations where increased border controls must logically be focused are the numerous border entry points. International situations and other trends may result in a strong immigration enforcement policy and a federal government decision to adopt a universal immigration border check before a customs review, as is now done by the USA. This new focus would in all liklihood involve the installation and use of computer-based travel document readers at border entry points. The automated checking process could conceivably extend so far as to include a requirement to call up stored images to check doubtful passports, or even the automatic display of all passport images as passports are scanned. In any case adoption of an immigration focus would have implications for the PPO and the accessability of its data and likely its graphics resources.

Federal-Provincial Cooperation.

Within Canada, the recognition of the need for more accurate verification of information for passport applications could encourage the sharing of information between provinces and the federal government. For example, links might be established to data bases such as birth and death registries maintained by the provinces. These initiatives would again will have an impact on PPO computer

[3] pg 1, *The Globe and Mail*, October 17, 1991

information systems planning.

Possible Integration with Similar or Related Programs.

Programs are already underway at several Canadian government departments to utilize digitized imaging for identification documents. Immigration Canada has a pilot program underway to print visas with digitized black and white images; the Secretary of State (Citizenship) is now in the proces of tendering for a system to produce identification cards with colour digitized images; and police departments across Canada are implementing identification systems utilizing digitized images. Within Canada, it is entirely conceivable that a need will exist to exchange images digitally with other organizations for identification purposes, or even to integrate federally controlled programs in some fashion.

Outside of Canada, immigration agencies are under the same pressures to control the inflow of illegal aliens that we see in Canada. A number of those countries are already implementing MRP and MRV systems - as enforcement policies are strengthened, Canada could well have to provide digital images or other types of check data on an individual demand basis as an identification service to its passport holders and international government partners.

All of the above scenarios are possible and credible, and imply very significant changes in the computerization of the PPO.

6. Emerging Technologies

The 80's have witnessed the development of many technological advances, particularly in the fields of computer systems and architectures. So great has the rate of development been that the "life cycle" of most commercial computer-based applications is said to be in the order of three years! This implies that upgrading to remain current must take place every three years or so, with the continuing evaluation and planning for such upgrading an important aspect of organizations which use informatics. In fact, a current management principle in support of regular strategic planning maintains that failure to institute regular planning simply means that the inevitable upgrade, when it finally must be done, will be every bit as expensive but less well planned and more traumatic for the organization than the continuous upgrade alternative.

Technological changes in computer systems architecture in the 80's are so great as to be considred revolutionary rather than evolutionary. Consider that the personal computer, so powerful and prevalent today in every work environment, was only first announced by IBM in 1981. At that time no one could guess what the future would be for the crude, slow and limited system that represented the first PC. Even IBM felt at the time that it would represent only a minor complement to its main business, yet it has fundamentally changed the computer industry and the modern work environment.

Advances in PC technology alone have been astounding. A high-end system today, perhaps represented by an Intel based 486/33 IBM AT clone, has more than 25 times the processing power and speed of the IBM AT system which it mimics and which was introduced by IBM in 1984 as an improvement to the 3-year-old original PC. More remarkable, the cost of such a system is not any greater than the cost of the original AT system. These trends are also evident in modern desktop workstations, which make available to individual users greater power and much lower prices than very large and powerful minicomputers that were being marketed in 1980. New versions of these workstations, with technologies such as "RISC" (Reduced Instruction Set Chips) and dense chip integration, show version to version improvements in speed measured in orders of magnitude rather than simple multiples.

This ubiquitous trend, which will continue through the 90's, has great significance

to the PPO and its strategic planning process. For example:

(a) Advances in technology will be adopted by individuals and corporations into everyday life. This may happen slowly but it will happen inexorably. As a consequence life in the 90's will be different from life in the 80's; technology will cause changes to informatics use, and will create demand for the application of new capabilities. The federal government itself as well as the public may be a source of demand for the use of new technological capabilities from PPO operations and data resources.

(b) The public, although concerned with privacy, can nonetheless be expected to show a high degree of acceptance of new technologies into their lives. Banking machines, computerized ticketing, and PC's in the home, school, and workplace are all examples of this trend. None of these developments are very old but are quite widespread now. The PPO should therefore not expect negative reaction to thoughtfully planned changes to its use of modern informatics and related technologies into their operations.

(c) Dealing with the pace of change for informatics and technology is best done by a proactive and regular process of life cycle management for all technologies and systems introduced. This process should incorporate strategic planning and budgeting for upgrade and replacement. If this is not done, the PPO, like all organizations using informatics technology, will eventually be exposed to an inability to provide capacity and new services which management and the public will come to expect.

The remainder of this section describes the main technological thrusts which will have a significant impact on the PPO in the 90's.

6.1 Document/Image Management.

Document/image management is potentially the most significant emerging technology that will affect the Passport Office in the next 5 to 10 years. Imaging has been

described as the "computers' new frontier" by Forbes magazine. [4] Although several technologies are closely related, this section will deal primarily with imaging - other sections dealing with printing, storage and communications technology must be considered part of the total document/image processing technology.

Imaging technology has been available for a number of years, with it's primary application to date being the scanning of graphic documents. Document input has until recently only been handled by OCR (Optical Character Recognition) devices, which usually placed strict limits on the format of document and type font (e.g. the Machine Readable Passport). More recently, systems are available which scan the input document as a graphic element, and which provide automation tools for handling documents in electronic form, including OCR reading of the text. Document processing tools provided with some systems include indexing, storage/retrieval, archiving, annotation (with voice, text, or graphics), linking of related documents, etc. "A fully-integrated document/image management solution may include an image database, text, graphics, and voice annotation, optical character recognition, text search and retrieval, facsimile transmission and receipt, plus integration with mainframe applications, scanners, image printers, and optical storage."[5]

The effect of this technology is to provide more efficient handling of documents, more effective management of document based systems and automated tools to integrate video, graphics and voice with the document handling functions. This technology will be the foundation on which passport issuance will be based.

Imaging is of critical import to the Passport Office in at least two key areas.

- Digitization of photographs, signatures and other identification features for storage, processing, output onto passport documents, and later recall for comparison purposes.

---

[4] *Forbes*, p. 257 - 264, Nov 26, 1990

[5] *Sun Microsystems, Inc. Document/Image Management Portfolio*, Sun Microsystems, April 1990

- Document handling and management systems for processing passport applications (including integration of digitized photographs, signatures and other identifying characteristics) and archiving.

Although digitization techniques have been in use for a number of years, the recent trends that have had most impact are:

- improved OCR software to enable reading of many different fonts, including hand printed text, and text "zoned" by an operator after scanning.

- sophisticated software emulation of many document management functions (e.g. annotation, linking of documents, handling of documents as if they were paper files, file forwarding systems, etc.)

- lower product costs, especially in the area of optical disk storage devices and workstations

- increased computing power of PCs, workstations and minis and increased sizes of optical disk storage systems.

All of these trends are likely to continue in the future. More functionality will continue to be provided and at lower costs. The most significant cost reductions in future are likely to be in the area of optical disk storage systems, since this is a relatively new technology and since it is the most expensive component in most imaging systems today.

Although imaging may be considered an "emerging" technology, it has already found use in several government departments, some of them very similar to applications such as passport or identification documentation. The following examples were reported to the study team during the course of the review, and have been confirmed

as time and availability permitted.

- Secretary of State, Canadian Registration System (Citizenship documentation) - in the tendering process

- External Affairs, Protocol Office (ID cards and special diplomatic visas with digitized images)

- Immigration Canada (Machine Readable Visas with digitized B & W images)-in pilot phase

- Canadian Security Intelligence Service (ID cards with digitized colour images)

- Correctional Services Canada (prisoner ID cards with digitized colour images. Pilot phase at William's Head Penitentiary)

- U.S. Immigration and Naturalization Service (Machine Readable ID cards ("green cards") with digitized signatures, fingerprints, and colour images and future plans for document/image processing (May '92) - 2 M cards per yr.)

- U.S. Department of State (Machine Readable Visas with digitized B&W images)

- Consumer & Corporate Affairs, Patents Office (in tendering process - imaging of documents, OCR scanning of imaged documents, archiving of extremely large digitized files)

- Consumer & Corporate Affairs, Lobbiest Registration Branch ("nearly paperless office", imaging & filing of all lobbiest registrations - 15,000

- 20,000 files, free format documents; no OCR)

- Ontario Ministry of Consumer & Commercial Relations, Vital Statistics (births, deaths, marriages, divorce registries - imaging old archive - 11 million documents; imaging new entries + manual data entry - no OCR; "re-engineered business into paperless activity")

6.2 Communications Technology.

Communications technology will be closely integrated with any and all other technologies used in future passport systems. Communication services are available today which would allow transmission of virtually any type of information, including images (e.g. digitized photos, signatures and other identification features) and application history, to most passport issuing locations in the world at relatively low cost. Communications facilities can easily be established within an office and between all offices, missions and headquarters. It is conceivable that communications with other sources and destinations may be desirable in the future; for example to or from police computers, provincial registries, and Immigration Canada.

Communications technology can be utilized to provide sharing of all types of information between passport office users whether locally or internationally located. It can facilitate the efficient sharing of resources between workers in a single office; it can more completely integrate various steps in handling passport applications with data that is centrally available; and it can make the same information accessible to all offices, regardless of location.

Communications will be of strategic importance to the Passport Office in many ways.

- Transmission of images from a master data base for confirmation of identity.

- Transmission of information to a central data base for immediate checking of security related issues (e.g. PCL, Master Index, Guarantor lists, etc.)

- Transmission of passport data and image information to a remote site for preparation of emergency replacement documents.

- Transmission of passport data and image information to a local or remote site for preparation of renewal documents and return of updated image and data to the central data base.

- Transmission of application information to a central system for archiving.

Future developments in the field of communications are being driven by the bandwidth requirements and the connectivity requirements of distributed processing, imaging, and LAN interconnection. "Image processing is already very or moderately important to over 50 percent of the enterprises surveyed" according to one source.[6]

- FDDI (Fibre-optic Distributed Data Interchange) utilizing fibre optic cables and transmission speeds of 100 Mega bits per second will become common for interconnecting multiple LANs within a single building or adjacent buildings, and for higher speed transmission within a single LAN

- ISDN (Integrated Services Digital Network) services will allow integration of voice, data, and video communications over wide areas. ISDN services are now being installed by many North American and European telephone companies, and interconnections between them will be common.

---

[6] "Private Network Challenges and Opportunities for the 90s", Timothy Zerbiec, *Telecommunications*, North American edition, January 1991

- WANs will provide higher speed services at lower costs (measured as a function of speed). The currently common speed of 9600 bps will be supplanted by services based on 64K bps ISDN service. 1.5Mbps transmission between major offices will be commonly used.

- With the advent of OSI protocols, connections across LANs and WANs will become more standardized, with more connections between different software applications possible. The exchange of data will be facilitated.

- Network management facilities will become more widespread as standards proliferate (e.g. SNMP - Simple Network Management Protocol and CMIP - Common Management Information Protocol), making management of hybrid public/private networks feasible for less sophisticated users.

- Packet networks will eventually migrate to higher speed Frame Relay or Fast Packet systems built on ISDN backbone facilities.

6.3 Printing Technologies.

Current and developing computer-driven printing technologies can add to the security of the passport document while simplifying the process of assembling the passport document. Typically, an image is printed as lines of very small dots - the quality of output is primarily determined by the number of dots printed per inch. The more dots - the better the image. Black and white printing is achieved by printing black dots on white (or other colour) paper. Colour printing is achieved by printing a mixture of three primary colours (yellow, magenta, and cyan) which are blended into a colour image by the human eye.

By printing the passport holder's image directly onto the passport, security is enhanced in several ways. Elimination of a glued-on photograph prevents replacement with another photo; retention of the same image in a computer data base allows comparison of the printed passport image with the original image on-file.

Also, printing of the image directly onto the passport page can simplify the labour intensive procedure currently used in gluing the photo onto the page.

A great variety of printer types exist today - details of each are discussed in Appendix B.3. They include black & white laser printers, colour laser printers, black & white and colour ink jet printers, die sublimation printers and colour thermal transfer printers.

Printer technology is being driven by the PC/workstation/LAN market and the users' need to have low cost, high quality output that is comparable to the screen output available on PCs and workstations. The current technological standard of 300 dots per inch (dpi) has proven satisfactory for output of printed text and line drawings, however, 300 dpi is generally not suitable for high quality image output where subtle shadings are required - this can be overcome with greater density of dots, or with continuous tone techniques (e.g. die sublimation).

Current trends are:

- The cost of colour printers is rapidly being driven downward by new developments and by market demand.

- Costs of B & W laser and ink jet printers have probably levelled off since there is little room for further decreases with prices now in the $1,000 to $3,000 range.

- Quality of image output is increasing with most manufacturers now offering 300 dpi minimum and many providing higher densities (400, 600 and 1200 dpi).

- The cost of special coatings and ribbons for colour printing is quickly dropping as quantities sold allow economies of scale. (Current costs can

run as high as $1.00 per page of colour output.)

- There will undoubtedly be a movement toward colour printing on plain (uncoated) paper. At the present time however, the only inexpensive printing technology that can produce continuous-tone image (die sublimation) does require special coating - it also has the added benefit of producing an image that does penetrate into the paper surface to some extent. However, those technologies that do not require coated papers (laser and ink jet devices) deposit their inks on the surface of the paper - a security issue that may have to be addressed by the Passport Office.

- The use of printers on low cost PCs and workstations has already driven printer suppliers to utilize a small number of common interfaces. This trend will continue. The benefit to users is the relative interchangeability of printers as better, faster, or less expensive devices become available.

6.4 Storage devices.

Large volume data storage devices provide an enabling technology - without the capability of these devices, it would not be feasible to consider storing images or documents on-line or in an automated archive.

The volume of data required to represent scanned images can be quite large. Typical colour head-and-shoulders images of near photographic quality require 20K bytes each (after compression); typical 8.5 x 11 inch documents scanned at 300 dpi require 70K bytes each. A simple calculation suggests that storage of one year's imaged photographs (1.2 million images at current production rates) would require 24 Giga bytes. One year's storage of digitized signatures might require 3 Giga bytes (1.2 million signatures at 2.5K bytes each). Storage requirements for imaged documents could consume 252 Giga bytes of space (assuming an average of 3 documents each for 1.2 million applications in one year).

Trends:

- Larger sized disks and larger jukeboxes as archiving use grows

- Lower prices as volume of product grows - currently the largest single cost in most archiving systems ($200K for 300 G bytes)

- New software compression algorithms may reduce storage requirements somewhat.

6.5 Software.

Trends in three key software areas present opportunities for the Passport Office

- The implementation of distributed applications is being facilitated by the acceptance of both formal and "de facto" software standards and the availability of software packages which implement those standards:

  - 5 or 6 industry standard formats for graphic images (e.g. TIFF, PCX, etc.) are in common use

  - DDE (Dynamic Data Exchange) is gaining widespread acceptance as a means of moving data between applications

  - The ISO (International Standards Organization) 7 layer model for Open Systems is gaining acceptance and formalized standards are being implemented (e.g. X.400 for E-Mail, FTAM for file transfer, EDI for electronic data interchange, etc.)

- The Optical Character Recognition (OCR) function has recently moved from implementation as firmware in a document reader to software in a PC or workstation. At the same time, flexibility and capabilities have been expanded to give reliable recognition of many different character fonts and sizes - 99.5% accuracy is claimed by at least one vendor. [7]

- Relational data bases have evolved over many years and can readily provide the ability to link data in virtually unlimited ways - thus allowing functions that require a great deal of flexibility in handling different data fields such as those involved in a passport application. Recent developments allow inclusion of graphic elements (images) as a supported data type in some relational data bases (e.g. Informix). In fact, in a survey of 17 PC based data base management packages, 7 have explicit support for graphics in industry standard formats. [8]

6.6 Other Technologies.

One technology with potential to significantly change the system of physical passport books is the "smart card" or document with an integrated circuit ("chip") imbedded in it. These cards are now in common use in some European countries as credit/debit type cards. The chip can store information about the cardholder which can be read by a machine. Additional information can be written into the chip by the same machine.

It is conceivable to think of a passport with similar technology. The chip could contain biometric data about the holder which would have to match the image on the data page. Positive confirmation of biometric data could be accomplished by matching fingerprint or signature data from the chip with the cardholder's own fingerprint or image. It is reported that a system is currently being piloted in Holland which allows frequent business travellers to use a card for automatic

[7] *DOS Resource Guide*, IDG Communications, issue No 2, 1991

[8] ibid

identification upon arriving in Holland - the card holder inserts the card into a machine and presses his finger against a reader which then compares the two biometrics; if the comparison is verified, the traveller is automatically gated through immigration.[9] For further use as a travel document, visa information could be written electronically into the chip.

As an additional level of security, the contents of the chip could be checked against the original image stored in a database at the Passport Office by simply transmitting a checksum from the chip and having it compared to the same checksum in the image database.

While such a card might have significant impact on the ways passports are used by travellers and immigration departments, this technology would be entirely feasible for the Passport Office if supported by the previously described imaging, communications, printing and storage technologies. The only addition would be some means of writing the information to the passport chip, and the inclusion of the chip in the passport. Immigration departments desiring to utilized these features would have to equip themselves with appropriate readers (already commonly in use for banking applications).

---

[9] Reported by Mr. Jerry Webster, Director, Alien Documentation, U.S. Department of Justice, Immigration and Naturalization Service.

7. Special Passport Security

In section 4 and elsewhere, reference was made to the potential for increased Canadian and international focus on the reliability and integrity of passports and other travel documents. This focus may be intensified not only by illegal immigration, terrorism, and drug trafficking concerns, but also by the forseeable general availability of technologies to forge passports. The ability to counter these concerns with technology that is becoming commonplace, such as efficient wide-bandwidth communications, digital image storage and retrieval, and new printing technologies, can be expected to create new demands for better security for passport issue and authentication.

The Passport Office, like its counterpart organizations elsewhere in the world, are facing what can be called the "passport fraud cycle". In essence this consists of a "motivation loop" for those individuals in society who wish to acquire a fraudulent passport. This is represented diagramatically illustrated in figure 1 on the next page. Essentially an individual seeking a fraudulent passport has a fundamental choice between counterfeiting a new or existing passport, or trying to have an official passport issued in fraudulent circumstances. If too much risk is associated with trying to use a counterfeit passport, for example by better electronic on-line checking, then increased effort will be placed on having the PPO issue a "valid" passport to an applicant posing as a fictitious or dead citizen. The reverse is also true.

At the present time, unfortunately, little coordinated attention seems to be paid by Canada to this joint issue. Passports are issued with care amnd attention to detail, with many disguised security features in the passport document itself, but these are seldom if ever checked at Canadian entry border points. Canada has a Customs and Excise focus at its borders, and passport security features do not seem to be a priority. In this sense, the extensive security features built into the document itself seem pointless. Other countries, such as the USA, do read the machine-readable section of the Canadian passport, but this is only to facilitate a quick check for known undesirable foreigners on the US list; they do not verify the authenticity of the passport.

THE PASSPORT FRAUD CYCLE

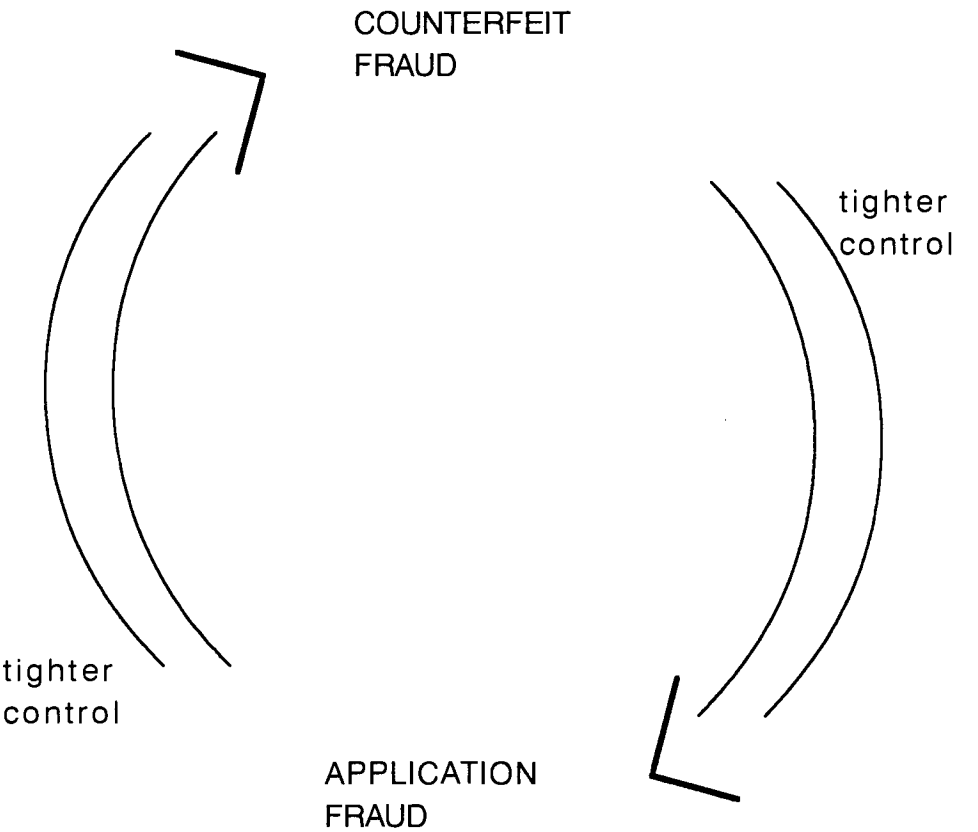


Figure 1

Passports have recently been reported by the media to be relatively easy to obtain from the Passport Office. This has largely resulted from the use of fraudulent "birth certificates" from provinces, since the PPO must rely on documentation sent and can really only verify the existence of the town and perhaps the name and birthdate in exceptional circumstances. It is known that a number of operational initiatives are being implemented which will improve this situation, but it is clear that ultimately much better computerized links with provincial data bases and guarantor files will be necessary to shore up this aspect of the passport fraud cycle.

A strategic focus on both elements will eventually be necessary to raise the true security, integrity, and reliability of the passports issued by Canada. This security of documents will be realized with two types of support:

- **Intrinsic security**, involving the existence of a passport which has been authenticated carefully before issue, and which contains security codes and inks, probably digitized and computer generated pictures, signatures, and other difficult to copy elements; and

- **Extrinsic security**, involving the common use in Canada and perhaps elsewhere, of on-line authentication as the situation warrants. Such authentication may involve picture and signature display on the screen of the Immigration officer, as required.

Faced with difficulties both in obtaining a "valid" passport through a fraudulent application, and with the real probability that detection through the use of a forged passport will result, the passport fraud cycle can be effectively countered. Lack of sufficient attention to both facets of this problem can, however, considerably weaken the effectiveness of the program. This fact, along with the awareness that technologies to deal with the problem properly, can be expected to come increasingly into view by various governments during the 90's. As a result, the evaluation of alternate means are the proper strategic focus of the Passport Office.

In figure 2 are shown some of the ways in which the intrinsic security of the passport may be augmented in the next few years.

CANADA

P CAN RK127127

BLTXPHK

MARY JO

CANADIAN/CANADIENNE

29 NOV /NOV 44

F VANCOUVER CAN

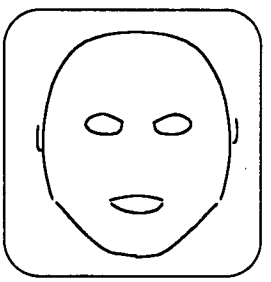
21 SEPT/SEPT 98 HULL

21 SEPT/SEPT 03

LESS SECURE SCENARIO

No biometrics
Not machine readable

CURRENT PASSPORT



CANADA

P CAN RK127127

BLTXPHK

MARY JO

CANADIAN/CANADIENNE

29 NOV /NOV 44

F VANCOUVER CAN

21 SEPT/SEPT 98 HULL

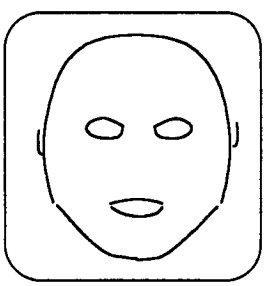
21 SEPT/SEPT 03

P<CANBLTXPHK<<MARY<JO<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

RK127127<4CAN4411293M9309212<<<<<<<<<<<<<<<<<<<00

INCREASED SECURITY SCENARIO

Digitized image
Digitized signature
On-line recall of image & signature from data base
Electronic componant with on-line checks
Finger print?



CANADA

P CAN RK127127

BLTXPHK

MARY JO

CANADIAN/CANADIENNE

29 NOV /NOV 44

F VANCOUVER CAN

21 SEPT/SEPT 98 HULL

21 SEPT/SEPT 03 Mary Jo

P<CANBLTXPHK<<MARY<JO<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

RK127127<4CAN4411293M9309212<<<<<<<<<<<<<<<<<<<00

Figure 2

The top example shows a pro-forma older style passport which of itself contains little reliability and could be readily forged. The lack of a photo and other coded data would not be considered adequate today.

The current passport is shown in the middle picture, containing the photograph of the holder and a machine readable zone which records the passport number along with some "biometric" and control information. (The term "biometrics" refers to data for an individual which is basic in nature, unchangeable, and not particularly sensitive. For example, one's name, picture, date of birth, and signature are all biometric information elements.)

In the lower picture is shown a passport ID page which contains a variety of options which may become the norm during the 90's. The technology to do this exists today. Special features include:

- A digitized image first captured by the Passport from the picture submitted or from a video camera image capture. In any case, the image digitally imprinted on this page is the same that can be retrieved from central data files for renewals or inquiries.

- A digitized signature block, machine generated after capture from the application form in a similar manner to the above. This signature could also be called up to screens as a result of renewals and inquiries.

- An integrated read-only chip with special authentication features such as control counts and other self-checks. These features can be readily verified by appropriate readers, thereby directly increasing intrinsic passport security. The information on the chip can also be readily checked against central data bases for excellent extrinsic security protection as well. In this latter mode, note that no data on the passport holder need be released for authentication, only the control checks. Use of the chip, albeit expensive today, can render passports virtually non-counterfeitable with proper checking procedures.

- Other features may be included, such as digitized fingerprints which could again be retrieved from central data sources. This feature might be considered too controversial to incorporate quickly.

Special readers used at border points could check the above enhanced security features along with special inks used (visible only in the near-infrared). Where warranted, additional call-up of equivalent file images could be made, facilitating detection of fraudulent use.

8. The Strategic Relevance of Passport Office Data Recources

As the role of the PPO expands in the 90's to support international security issues, and as the data bases of the PPO are set up with more comprehensive and accessible information, these data resources may themselves become of strategic importance to the government. The possibility of this occurrence is real, given the expected widespread growth and acceptance, and expectations of managers, of on-line systems and networks.

The issue is important to consider as an entity in itself, resulting in focus and planning for the design of the data base as a potentially shareable resource rather than simply a support for PPO operations. There is an important distinction between the perceived uses and the resulting design of the two scenarios.

If international pressures for security result in the requirement for on-line passport authentication, perhaps at least at Canadian borders with an Immigration rather than Customs focus, and for Canadians travelling out of Canada, then the PPO will undoubtedly be involved in restricted on-line access to its files for passport number, base data, and picture/signature data on request. Such operation would represent a significant new role for the PPO function and data resources.

The new data bases may become of interest to governments in other areas as well. For example, a close (2-way) association with police files may become expected, as could common application with Immigration. Equally important to consider are limited access rights, bilateral, with certain political allies such as the USA and the UK. Although it is difficult to imagine a wholesale sharing of data files with foreign countries, it is not inconceivable that certain countries (or perhaps even the UN) sponsor a shared access data hub for international authentication of passports for citizens of member countries. Similarly, international airlines may also be interested in data access. Current and forthcoming technologies will make such data sharing possible. The PPO should design its future data base resources with such possibilities in mind, so as to facilitate such programs as they arise, or even suggest them.

The issue of data privacy must be raised in such considerations. Certainly if a trend can be detected in the early 90's it is that individuals are becoming **more** sensitive

to their rights to privacy of their personal information in large data bases, even as technology for on line access and computer-based services becomes widespread and accepted. Even today consumers happily read out credit card data over the telephone to mail-order shops, but resent the use of this data for subsequent junk mail and even marketing based on the credit ratings determined as a result.

In the case of passport data, privacy of much of the information will remain an issue, in all liklihood preventing sharing and copying of data files and implying security for any access privileges granted to other agencies. However, in terms of biometric data (picture, signature, birthdate, fingerprint ?), the question can be raised regarding the violation of privacy, if any, that would be caused by permitting access to this data to authenticate a passport presented by the bearer at an Immigration point (Canada, USA, etc.). It must be borne in mind that the bearer is already voluntarily revealing this data to Immigration officers, since it is contained in the passport itself. If the Immigration officer calls up a display of file picture and signature for the bearer, it may not be realistic to claim that the display of equivalent biometric data from central files is a statute violation of privacy.

In the case that privacy statutes nonetheless restrict such biometric file access, the PPO may seek out an early implementation of the passport chip technology mentioned previously. This chip would store authentication information to confirm the data on the passport in which it is contained, and also contain certain control codes. The authentication process would involve verification of passport data by local checking of the authentication information with secure algorithms, followed if necessary by verification of the control codes centrally. These steps would not violate privacy of personal passport data files.

These issues of privacy could be resolved by requesting all applicants to sign a limited waiver for the release of such information in those circumstances as a way of ensuring no liability for subsequent action. The results of strategic planning for the 90's by the PPO should resolve this question into consideration and perhaps result in the implementation of such measures for all data collected as soon as possible, in order to build information banks of accessible passport data prior to these new systems being installed. The time period for construction of a complete new set of passport files (of current holders) is 5 years.

9. Conclusions and Comments

Many suggestions have been made in the above sections regarding the increased strategic roles that may develop for the PPO and its operations during the 90's. These may arise from many factors, such as:

- Societal pressures - there will likely be increased volumes and security demands for passports and other travel documents, highlighting the activities, data integrity, and methodologies of the Passport Office.

- Enabling technologies - will provide many practical means for passport security enhancements, both intrinsically and extrinsically. These same technologies will unfortunately be available for fraudulent use and counterfeiting.

- Political pressures - Criminal counterfeiting as well as the growing need to identify fraudulent passports and their carriers upon presentation can be expected to create international pressure for new security developments in passport technology.

- Management awareness - of enabling technologies through common experience in everyday life with developments in personal computing, networks, client-server applications, and in credit card/banking systems, will create an expectation on their part for improvements and new measures for passport security and service. The PPO should be in a position to provide proposals to government managers for better security, on-line authentication, and modernized distributed facilities rather than react after the fact.

- Strategic integration - of PPO roles, systems and networks, and data resources into overall government strategic plans and operational programs can also be expected as a result of the above. This integration, which need not be organizational but rather operational in nature, will become a stronger motivation as the PPO modernizes its application systems into the 90's, and as government leaders are made aware of the potential

resulting from these changes.

It is important that the PPO take a focused long-term view regarding its future roles and mandates resulting from the above influences, and possibly others. Most of these elements involve the planned use of informatics technologies, which more and more are becoming inexorably tied to the fundamental strategic plans of many organizations. Informatics and evolving enabling technologies are inspiring change and social evolution, rather than being only tactical components in many programs. In the case of the PPO, informatics technology and PPO activities are so intertwined that this review had to deal with overall social and political issues rather than simply technology developments to carry out its mandate properly.

Some recent examples will serve to clarify the importance of a long term focus. As a result of the recent well-publicized set of articles in the Montreal Star regarding the ease of obtaining and using Canadian passports, the PPO has recommended a number of changes to improve security in the short and medium term. Many of these recommendations involve distribution of services in Canada and the reduction of mail-in and proxy applications. Other recommendations focused on security enhancement through pre-registration of guarantors and increased verification of documents such as birth certificates. A further important element is the HQ validation overseas of lost-passport reports, based on the Master Index as well as the Passport Control List (PCL).

None of these changes could be contemplated if it were not for the capability of modern informatics technology to enable their implementation. It would also have been preferable had a long-term planning process been in place to have identified, planned, and budgeted these changes in advance. Despite their regular planning processes to upgrade systems, security, and office locations incrementally in the normal course of business, the PPO was unfortunately forced to <u>react</u> to the larger issues that arose rather than have forseen the need and be in the process of implementing the improvements that could have resulted from a broader long term planning program.

Of course hindsight is characterized by perfect vision, and the PPO is now in the process of implementing such programs. The PPO is also certainly not alone in its need for deliberate long-term focus. It seems apparent that the Government of

Canada itself, neither alone or in cooperation with the provincial governments, has properly integrated and planned its strategy for citizen and resident identification and immigration. For example, the intrinsic passport security features built into the current passports issued by Canada have for the most part been designed through ICAO MRP committees and discussions, as well as by the PPO itself, but with little evident operational participation of other government sources. The features are rarely if ever used by Immigration at border posts, and in fact Canada still has a Customs orientation at its borders, undoubtedly facilitating fraudulent entry.

There is also little attention paid to passport authentication by Canada, even though Canadian passports have a machine readable zone (MRZ); the US government uses passport readers and an on-line systems access to identify undesirables and to track travel by citizens and foreigners. (Ironically, the readers used by the Americans at many border points to read the MRZ are devices manufactured by a Canadian company, AIT Advanced Informantion Technologies Corp. of Nepean, Ont.) At the present time, the government, with the recent recommendations made by the PPO, are focusing on reducing application fraud. As was pointed out in section 7, this will only deal with one side of the Passport Fraud Cycle; to counter the problem properly attention must also be paid to counterfeiting and usage fraud detection.

These do not appear to be integrated in the strategic concrns of the gavernment at present, but it is unreasonable to assume that this situation will exist for long. The Passport Office must therefore forsee this eventuality in its internal planning process.

The needs and benefits of long-term strategic planning for informatics can be summarized as follows.

Rationale for Strategic Planning for Informatics

1. Deliberately focuses the attention of an organization on its objectives, opportunities, priorities, and resulting informatics (and other) plans for the future. Provides a framework for detailed planning and budgeting.

2. Clarifies for all staff and management the long range strategy and plans of the organization such as the PPO, and avoids fear, resistance, and confusion.

3. Permits the organization to take advantage of appropriate technologies at appropriate times to improve business and products/services. Facilitates planned technological change in place of reactive and typically overdue change.

4. Maximizes the investment of limited financial and personnel resources in planned and prioritized developments.

5. Minimizes panic and wasteful reactions to unforseen events and demands. Greatly increases preparadeness.

6. Provides a logical and controlled context for life cycle system and application upgrade.

The last point above mentions life cycle management of an informatics program. This is highly recommended to the PPO as an important management tool tied to strategic plans for informatics. Reasons for this recommendation include the following elements:

(a) Permits a long range strategic plan for informatics to incorporate system and application upgrade for obsolescence as well as other factors such as demand growth, need for new technologies, etc. Termination of a life cycle is another justification for budgeted change, which frequently in a proper planning environment will be synchronized with the introduction of other desired improvements.

(b) Aids the organization in maximizing technological opportunities by permitting evaluation of newer techniques on a regular cyclical basis. The

same comment applies to the informatics applications of an organization, wherein opportunities for process re-engineering can be assessed on a proper schedule if the life cycle is pre-determined.

(c) Facilitates the budget process in a long range strategic planning process. Absence of proper system replacement budgets in multi-year forward plans create many problems when change is finally necessary.

(d) Actually saves money in the long term, since upgrade or replacement of all systems and applications must eventually be done in any case. This usually incurs much greater cost if done as a short-term or panic program, and often does not result in the most effective results for the organization.

In conclusion it seems apparent that the exploration of appropriate strategic planning directions for the Passport Office must take into consideration not just the passport application processing and printing tasks which is the principle focus today, but rather the following:

- The growing significance of the passport in international circles, including the criminal element, for travel and identity in an increasingly sophisticated global environment.

- The significance of the passport to Canadian Immigration programs, particularly as these may change in focus in the next 10 years.

- The great impact of rapidly developing technologies which will create expectations for passport access and security controls, since they can so readily be accomplished.

In other words, the Passport Office is not simply a publishing shop, but rather

represents a significant government program that can be expected to have increased government attention during the 90's. Recent public events would tend to lend credence to this statement. Similarly, the PPO is also not in the "computer business", but must realize that informatics represents not simply a tactical resource but rather one which is fundamentally important to the definition and performance of its mandate. Technology enables an otherwise off-line and administrative process to become a provider of essential services of considerable sophistication for the needs of the next decade.

If the PPO sees its mandate in this potentially wider scope, as predicted by the results of this review, then its informatics plan must in turn be fundamentally restructured to accomodate the new mandate. At the very least, the PPO should act to improve its preparedness level for many of the possible changes noted in this report. In fact, a good strategic direction will permit the PPO to become proactive within the government in suggesting beneficial program changes based on new technological possibilities. It is submitted that this is the responsible role of any modern organization.

In a later section of this report, the framework for a multi-year strategic informatics plan are specified for the PPO, involving two different possibilities. A cost program for each is also incorporated given basic cost structures researched during this study. In order to give better focus to these strategies the next sections discuss the present systems operation of the Passport Office and what the PPO might be in several years' time.

10. Present Passport Office Systems

Appendix A to this review contains a detailed description of the fundamental components of the present informatics operations of the Passport Office. Special emphasis is placed on the passport production system, including a procedural flowchart which facilitated understanding of the current process. Both HQ and typical regional precedures are included.

The present usage of informatics in the PPO consists of a sound application set and computer systems base, and is typical of designs origination in the late 70's and early 80's. PC's have been built into the processes, but most of the operation is not truly on-line. In particular security update information in condensed form is often sent by floppy disk to outlying posts, with considerable delay, resulting in some passport issuance done in the absence of current check files. A much more on-line orientation for PPO operations is a basic requirement reognized by PPO systems officials.

11. The Passport Office of the Future - A Scenario

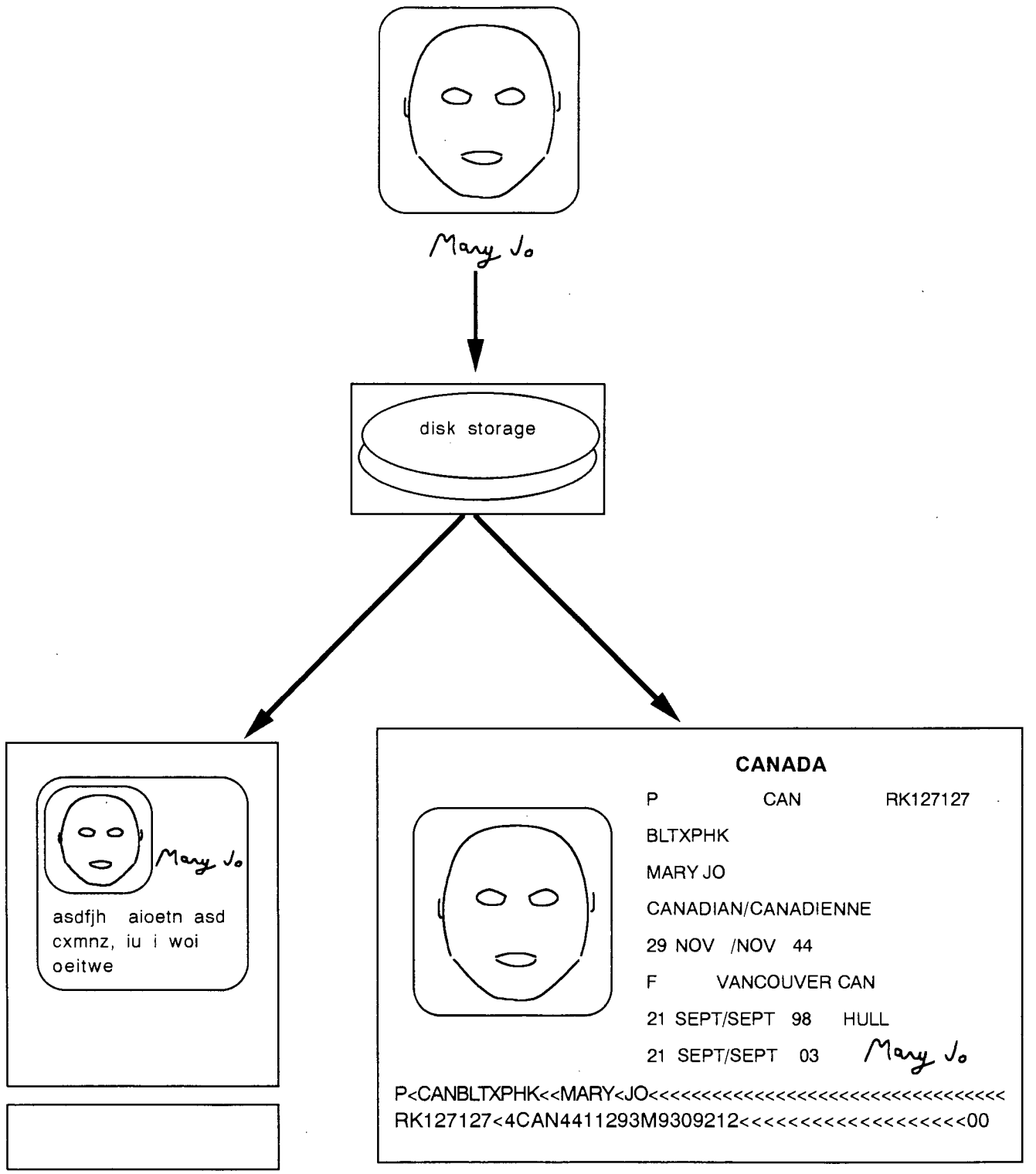
This section is intended to provide an overview of the technologies used in the PPO in future for the processing and authentication of passports. The section is not intended to be a review of all informatics to be used by the PPO in the planning time frame, nor to suggest in any way that a detailed design has been completed. Rather a descriptive operating framework has been put together using known technological dvelopments, in order to provide a sense of reality to the reader in understanding how it could evolve. Similarly, cost estimates for different components are included, mainly for budget sizing and eventual incorporation by the PPO as appropriate into the strategic plan framework to follow in section 12.

11.1 Operation

The following is a hypothetical description of a passport system as might exist five or ten years from now, utilizing equipment and technologies that are presumed to be readily available at that time. Certain operations or features that may currently be deemed unacceptable for socio-political reasons, such as the use of fingerprints, are included in the case of possible changes in social acceptability - they are not critical to the basic scenario described.

The applicant:

The applicant may be asked to sit in front of a video camera, have his or her image digitized, sign an electronic tablet, have his signature digitized, and put their thumb on fingerprint reader for a digitized fingerprint. All of these biometrics would be recorded for reproduction on the passport and for later recall from the computer as necessary for authentication of the passport document according to accepted security practices at that time. See figure 3 on Page 44 for a pictorial description of this procedure (shown for pictures and signature only).



BIOMETRIC IMAGING, STORAGE, PRINTING & RECALL

Figure 3

The applicant might fill out a "form" with personal information on a keyboard & screen or electronic tablet (it will still be necessary to have a means of processing paper based or electronically transmitted applications from remote areas).

The applicant might then sign a release form (via electronic tablet if allowed by law) authorising vital statistics checks and release of biometrics to foreign countries for passport authentication purposes.

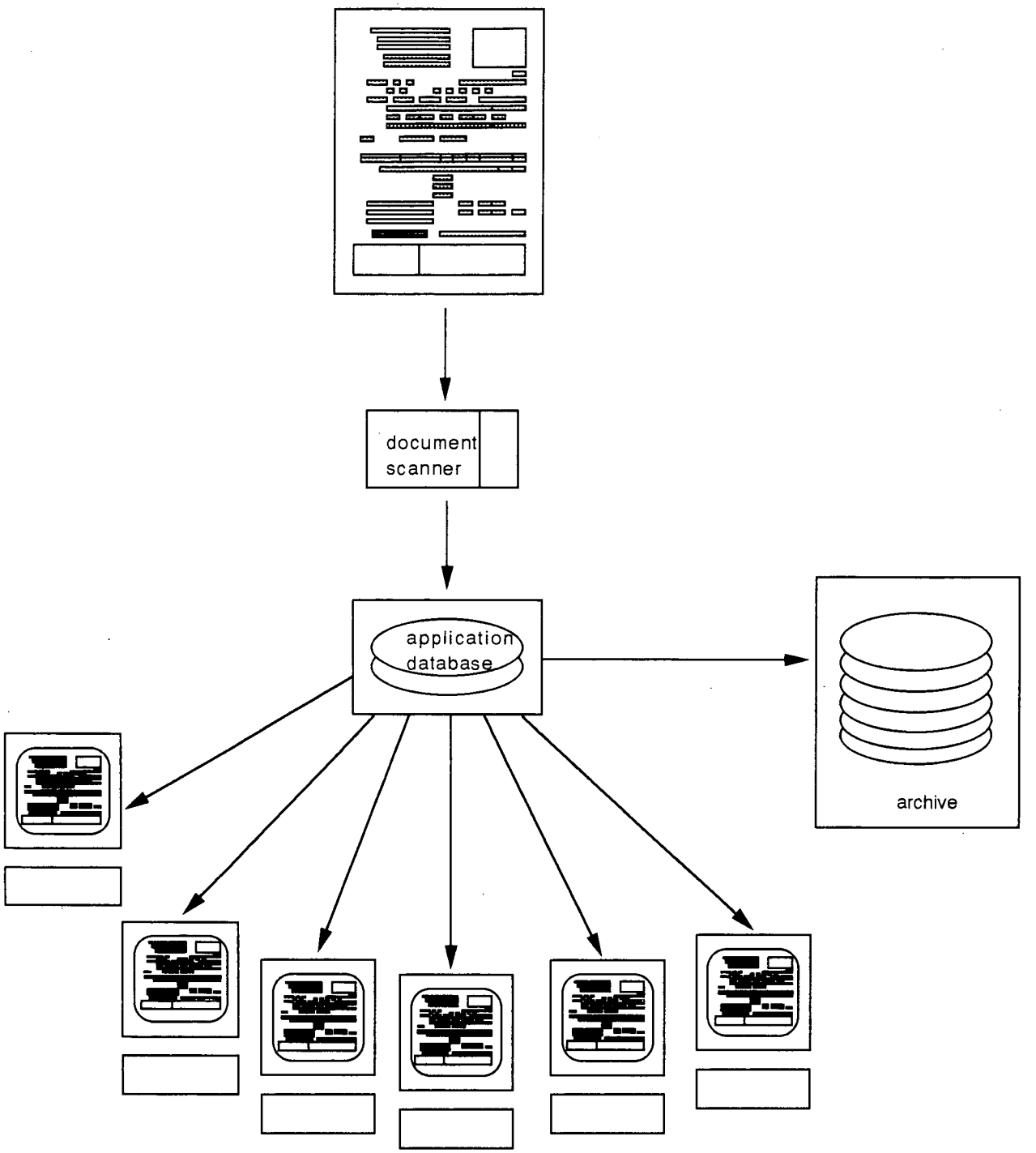
As is required at present, the applicant will probably still be required to submit documentary evidence - birth/baptism certificate, Declaration of Guarantor with signature, etc.

The passport office (application processing):

As personal data is entered, automatic checks could be done on previous passports, PCL and other watch lists. Any matches or alarms could be resolved by an examiner on the spot (for the majority of cases).

Figures 4 (page 46) and 5 (page 51) show schematically how the application captured in digital form and linked to biometrics is centrally available and automatically routed to various work stations as required. All stations are connected on local area networks to the same resources and common data files. A supervisor's station can review undue time delays and be automatically called in problem cases. In these latter circumstances the application would appear in the supervisor's queue, and on his/her screen, and be dispatchable from there to the next logical station. Work flow controls would be able to track, report on, and maintain schedule flow status of all applications.

Previous passport biometrics (head-and-shoulders image, fingerprint, signature) could be automatically brought to an examiner's screen within minutes as an aid to faster processing of passport renewals.



DOCUMENT IMAGING, WORKFLOW AND ARCHIVING

Figure 4

Guarantor lists could be automatically checked and a digitized signature of the guarantor could be automatically brought to the screen for on-the-spot comparison; guarantor statistics could be updated for off-line or back-ground analysis. Similarly, links to vital statistics registries might be automatically utilized to check the veracity of each application.

Digitized copies of complete previous application forms and supporting documentation might be available for recall by the Security section. (Similarly, complete digitized forms could be maintained for Certificate of Identity and Refugee Travel Document processing.) Direct links to FOSS, CPIC, PERS and other police systems might enable Security to perform more thorough checks. Data base searches by any data field could be possible - e.g. by address, by guarantor name, etc. - to allow analysis for security purposes.

The passport page could be printed with a digitized colour image, digitized signature, and digitized fingerprint; an imbedded chip (Write Once Read Many - "WORM") could also be written with the same biometrics and a polynomial checksum; the entire data/chip page would be laminated as it is presently.

If the application has been handled at a regional, local or overseas post, the above scenario could be identical in all respects, but checking of PCL lists, guarantor lists and other security data bases would be done remotely via telecommunication links to Ottawa. Any alarms or questionable applications might cause the entire application to be transmitted to Ottawa for Security or Adjudication personnel to handle.

After the application is processed all data might be automatically archived on optical disk. Applications could be automatically transmitted from remote sites for archiving.

The Passport Office (processing of requests for authentication and identification)

Requests might be be received on a telecom network from Canadian and/or foreign Immigration offices for authentication of passports by verification of checksums (i.e. a counterfeiting check recorded in the imbedded passport chip). Passport numbers and checksums would be received, compared with the data base, and the result forwarded to the enquiring agency within seconds (with no transmission of personal information).

Requests might also be received on the telecom network for Canadian and foreign biometrics checks (i.e. an identity check); complete biometric data might be retrieved from the archives and transmitted to the requestor via the telecom network within minutes after approval for release of information by Security.

Immigration counters

Where not equipped to read electronic chip or request electronic verification, processing would be similar to the current system - an immigration officer would do a visual check on image, signature, etc. Visas would be stamped manually as present system.

In highly automated locations, the passport holder might be asked to put his own passport through a reader, press his thumb against a fingerprint reader and wait a few seconds for a comparison with data in the imbedded WORM chip. If OK, an electronic visa might be written into a read/write portion of the imbedded chip, entry recorded in immigration computers, an entry gate opened and the visitor entered into the country.

If the self-reading entry process was unsuccessful, or if the immigration regime is more security concious, the passport would be handed over to an immigration officer who passes it through a reader. Electronics in the reader might automatically verify the polynomial check digits as a first level counterfeit check - the digitized image might also be displayed for a visual check against the image printed on the data page. Optionally, the immigration officer might request a quick verification of

electronic data in the WORM chip (by comparison of automatic on-the-spot calculation of polynomial check with polynomial check maintained in Ottawa). If further verification is needed, the immigration officer might request digitized biometrics to be displayed on his terminal via a telecom link to Canadian Passport Security, subject to approval by Passport Office security personnel.

11.2 Cost Estimates and Projections

These cost estimates apply to PPO configurations only, and not to immigration counter requirements, etc. Fingerprint and WORM chip technologies are excluded. Prices can be expected to reduce significantly during the 90's.

11.2.1 Central Site Costs. See Figure 5 for a configuration schematic.

Input workstation

RISC workstation	$25,000.00	
video camera & interface	$1,000.00	
document scanner	$7,500.00	
LAN interface	$1,000.00	
Total, 4 input workstations		$138,000.00

Examiner workstation

PC workstation, with colour monitor and LAN interface	$5,000.00

Adjudicator workstation

PC workstation, with colour monitor and LAN interface	$5,000.00

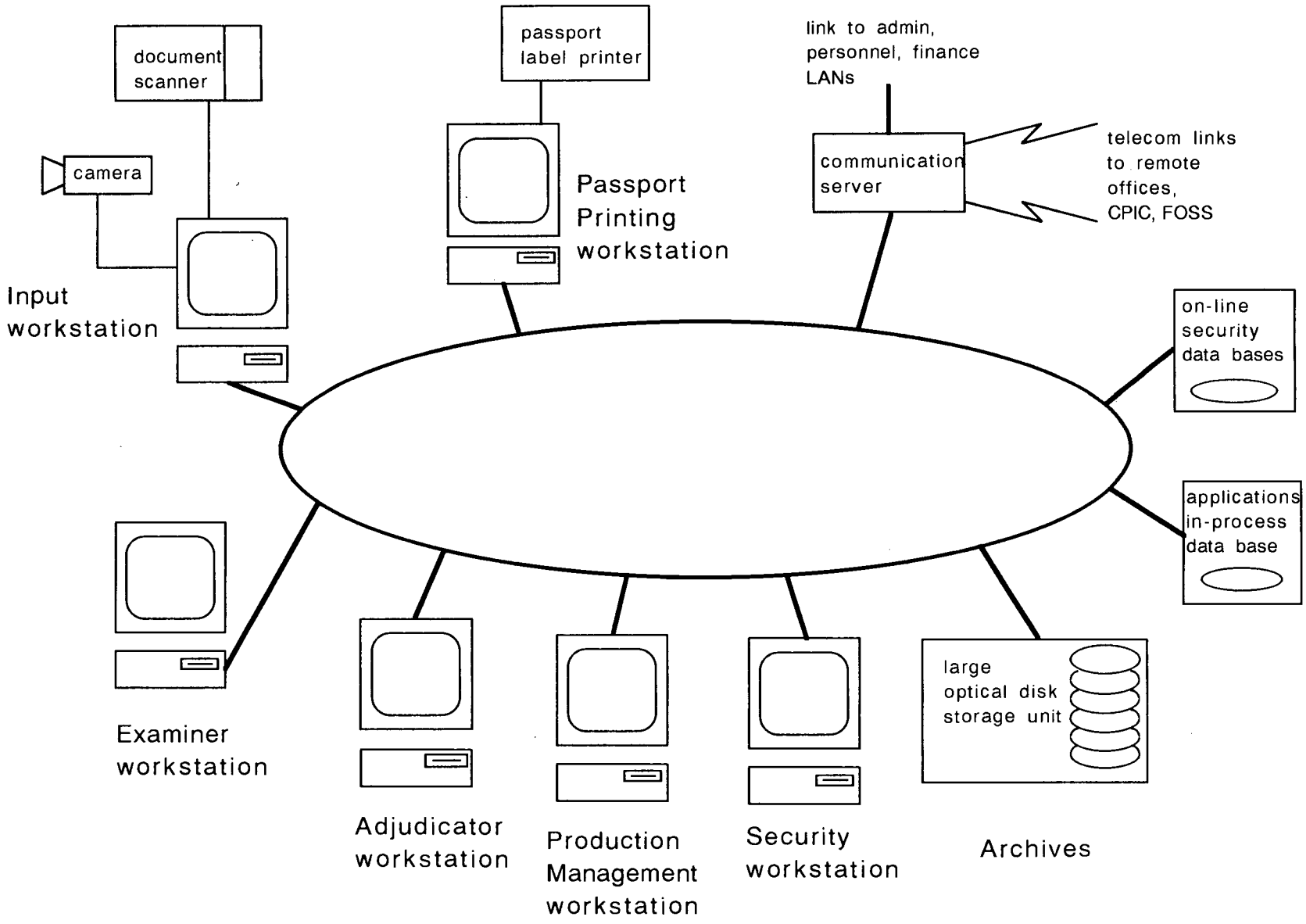
Production Management workstation

PC workstation, with colour monitor and LAN interface	$5,000.00

Security workstation

PC workstation, with colour monitor and LAN interface	$5,000.00

Total, 30 workstations for examiners, adjudicators, security, production management	$150,000.00



FUTURE IMAGE BASED SYSTEM,
CENTRAL SITE

Figure 5

Passport Printing workstation		
PC workstation, with colour monitor and LAN interface	$5,000.00	
Passport label printer	$7,500.00	
Total, 3 printer workstations		$37,500.00
Communication Server link to local admin LANs medium speed links (64K bps) to network	$30,000.00	
Total, communications server		$30,000.00
Security DataBase Server 1 G Byte magnetic disk	$13,000.00	
Application File Server 1 G Byte magnetic disk	$13,000.00	
Total, data base file servers		$26,000.00
Archive Data Base Server		
300 G. Byte optical disk jukebox	$250,000.00	
Total, 2 archive server		$500,000.00
TOTAL, CENTRAL SITE HARDWARE		$881,500.00

11.2.2 Regional Site Costs. See Figure 6.

Input workstation

RISC workstation	$25,000.00	
video camera & interface	$1,000.00	
document scanner	$7,500.00	
LAN interface	$1,000.00	
Total, 2 input workstations		$69,000.00

Passport Printing workstation

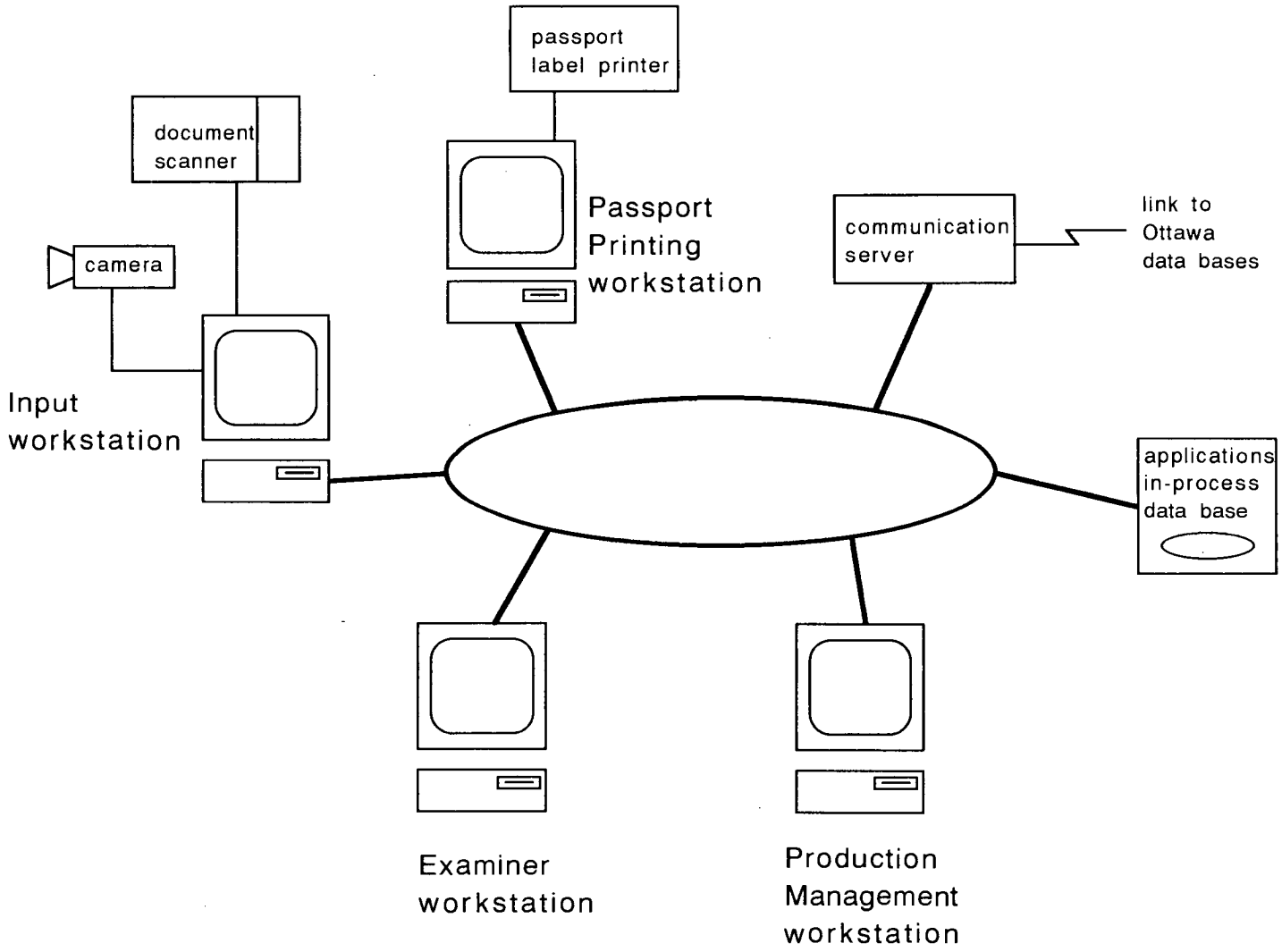
PC workstation, with colour monitor and LAN interface	$5,000.00	
Passport label printer	$7,500.00	
Total, 2 printer workstations		$25,000.00

Application File Server

1 G Byte magnetic disk	$13,000.00	
Total, data base file servers		$13,000.00

Communication Server

medium speed link (64K bps) to network	$15,000.00	
Total, communications server		$15,000.00



FUTURE IMAGE BASED SYSTEM
- REGIONAL OFFICES

Figure 6

Examiner workstation

PC workstation, with Colour monitor and LAN interface	$5,000.00

Production Management workstation

PC workstation, with colour monitor and LAN interface	$5,000.00

Total, 15 workstations for examiners, production management	$75,000.00

TOTAL, TYPICAL REGIONAL OFFICE HARDWARE	$166,000.00

11.2.3 Multiple Examiner Local Office Costs. See Figure 7

Input workstation

RISC workstation incl 1 screen	$25,000.00	
video camera & interface	$1,000.00	
document scanner	$3,000.00	
Total, basic & input system		$29,000.00

Passport printing

Passport label printer	$7,500.00	
Total, printing		$7,500.00

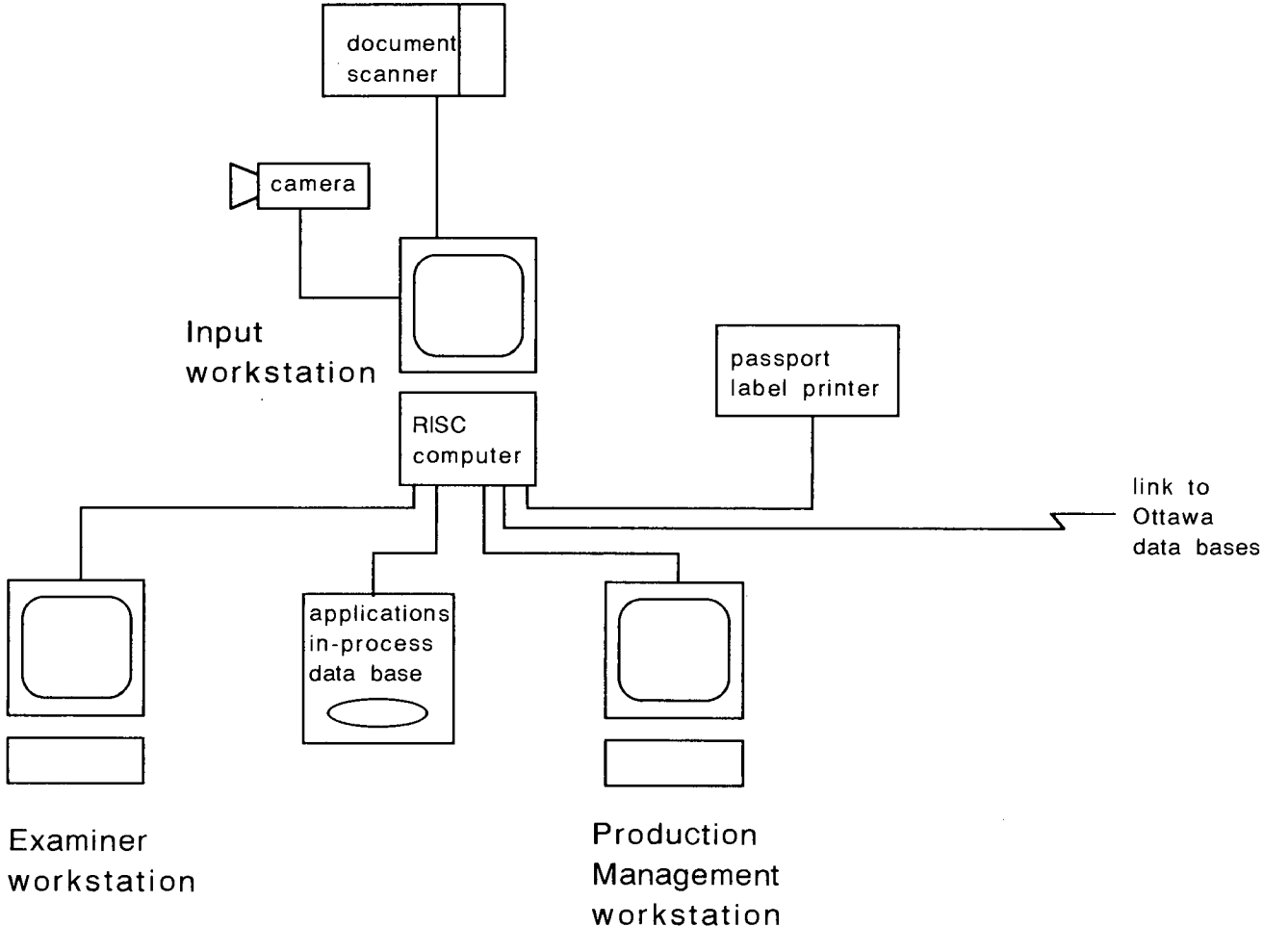
Examiner/management workstation

slave terminal	$2,000.00	
Total, 3 workstations		$6,000.00

Communication interface

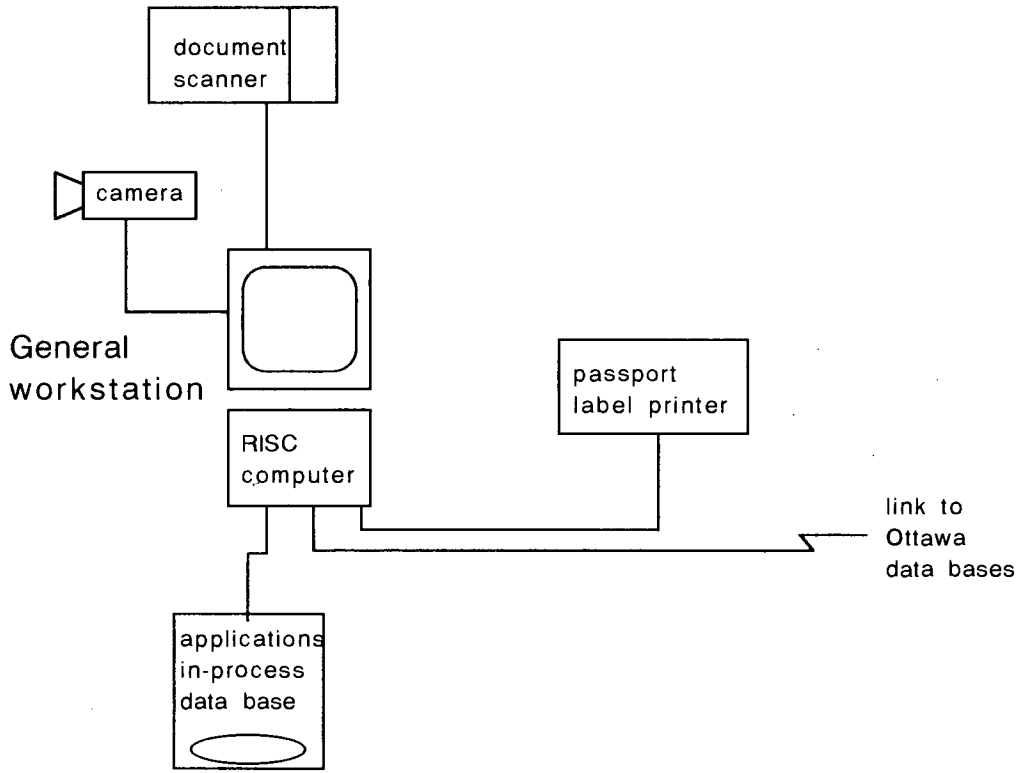
9600 bps to network	$1,000.00	
Total, communications		$1,000.00

TOTAL, MULTIPLE EXAMINER LOCAL OFFICE $43,500.00



FUTURE IMAGE BASED SYSTEM
- LOCAL OFFICES & POSTS

Figure 7



FUTURE IMAGE BASED SYSTEM
- LOCAL OFFICES & POSTS,
MINIMUM CONFIGURATION

Figure 8

11.2.4 Minimum Local Office/Foreign Post System Costs. See Figure 8.

Input workstation		
RISC workstation, incl examiners screen	$25,000.00	
video camera & interface	$1,000.00	
document scanner	$3,000.00	
Total, basic & input system		$29,000.00
Passport printing		
Passport label printer	$7,500.00	
Total, printing		$7,500.00
Communication interface		
9600 bps to network	$1,000.00	
Total, communications		$1,000.00
TOTAL, MINIMUM LOCAL OFFICE		$37,500.00

11.2.5 Hardware Summary

Central Site	$881,500.
5 Regional Offices at $166,000 ea.	$830,000.
11 Medium Offices at $43,500.00 ea.	$478,500.
22 Local/Foreign offices at $37,500.00 ea.	$825,000.
TOTAL ALL OFFICES.....	$3,015,000.

12. Getting There - A Strategic Planning Framework

In order to evolve towards a future PPO operation of the kind suggested, the PPO will be required to institute more formal and detailed planning exercises with its internal management, including review and agreement on its potential future role, mandate, and resulting informatics goals. This section is intended to provide a high-level framework for tasks and time frames that are suggestive of the possible results of such a planning exercise. The tasks and milestones are all expressed in a generic manner, since the study team could not attempt to provide a definitive statement to the PPO of its proper direction over the next several years.

The plans or implementation alternatives in this section are shown in the format of activity flow charts, showing basic precedence of major tasks to others and suggesting a time frame within fiscal years. A useful plan for the PPO, resulting from internal meetings on this subject, can also begin at this level to aid overall understanding and be subsequently fleshed out in much more detail as a result of further detailed planning and budgeting.

12.1 Implementation Strategies

Two possible implementation strategies are presented in the following material. The first and recommended strategy, strategy A, assumes that the PPO will advance to an informatics structure of the type described elsewhere in this report in a reasonable time period over the next 4 fiscal years. Biometrics capture for data base universality in the same time period would begin early, for later use with the integrated system. Strategy B, on the other hand, shows a more evolutionary path to a similar but more limited end point over a period of 5 years or more.

12.1.1 Strategy A

The aim of this strategy would be to provide an integrated approach and centralized control to the security, application processing, and archiving functions, on an

accelerated schedule while implementing new imaging technologies and utilizing telecommunications to link remote sites to Ottawa. This strategy assumes the technical goals are:

- Access to up-to-date data should be available equally to all users that are authorized by the Government, regardless of location, as quickly as possible. Realistically this applies to Canadian access worldwide as a priority.

- Expand current data bases for increased security

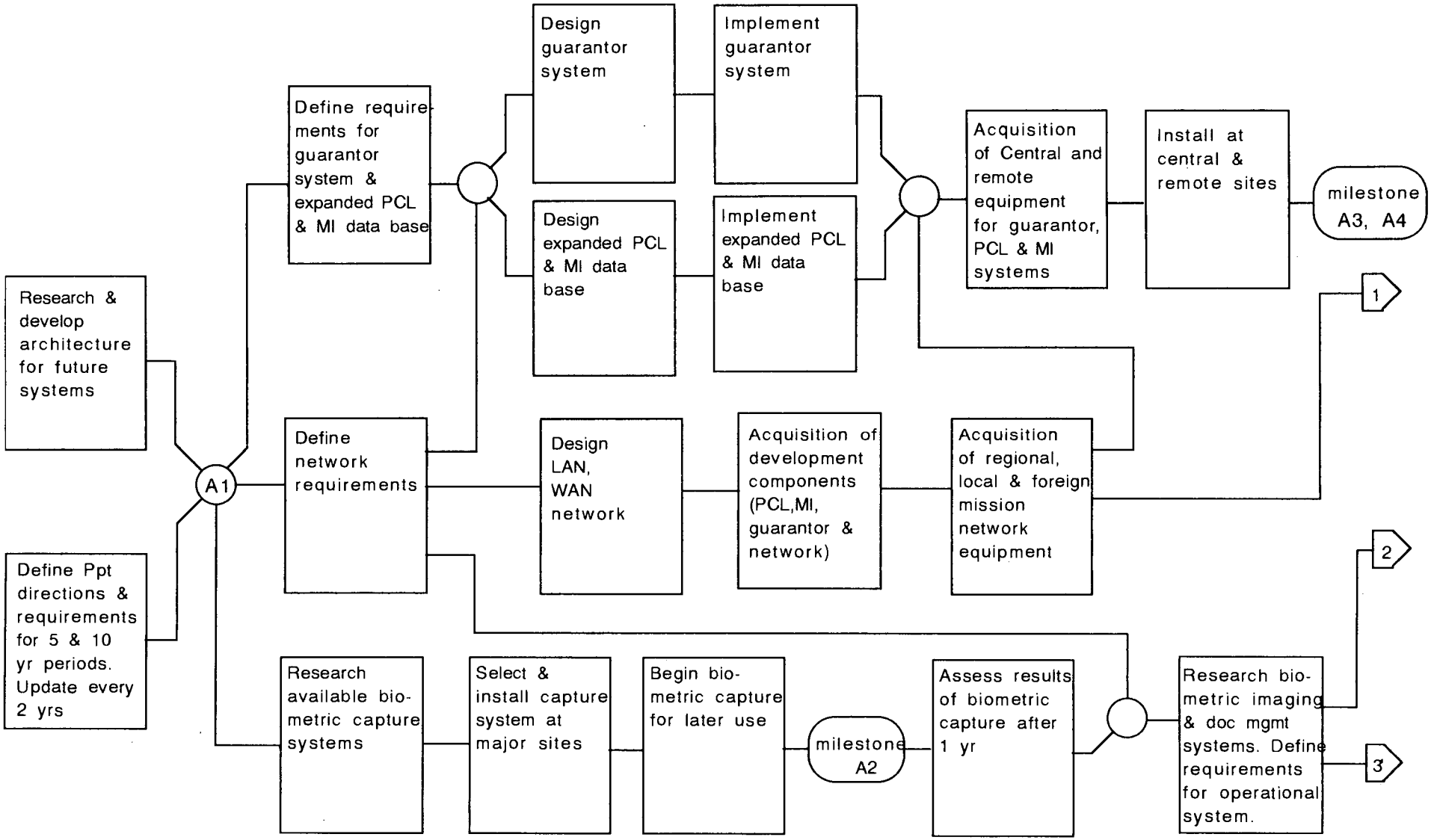
- Provide access to external data bases (Federal and Provincial vital statistics, police, Immigration, etc.), and provide controlled access to Passport Office data bases by other departments and agencies.

- Begin to capture biometric data in the near future so as to bring the data base up to a fully converted level by 1995/96. Utilize biometric data for production of passports by 1994/1995.

- Electronic archiving of biometric data will be required in conjunction with use in passport production.

- Provide imaging of documents and electronic "workflow" to handle increased volume of applications and improve efficiencies. Productivity gains would be realized in the minimization of paper handling and the resulting throughput achieveable with available PY's.

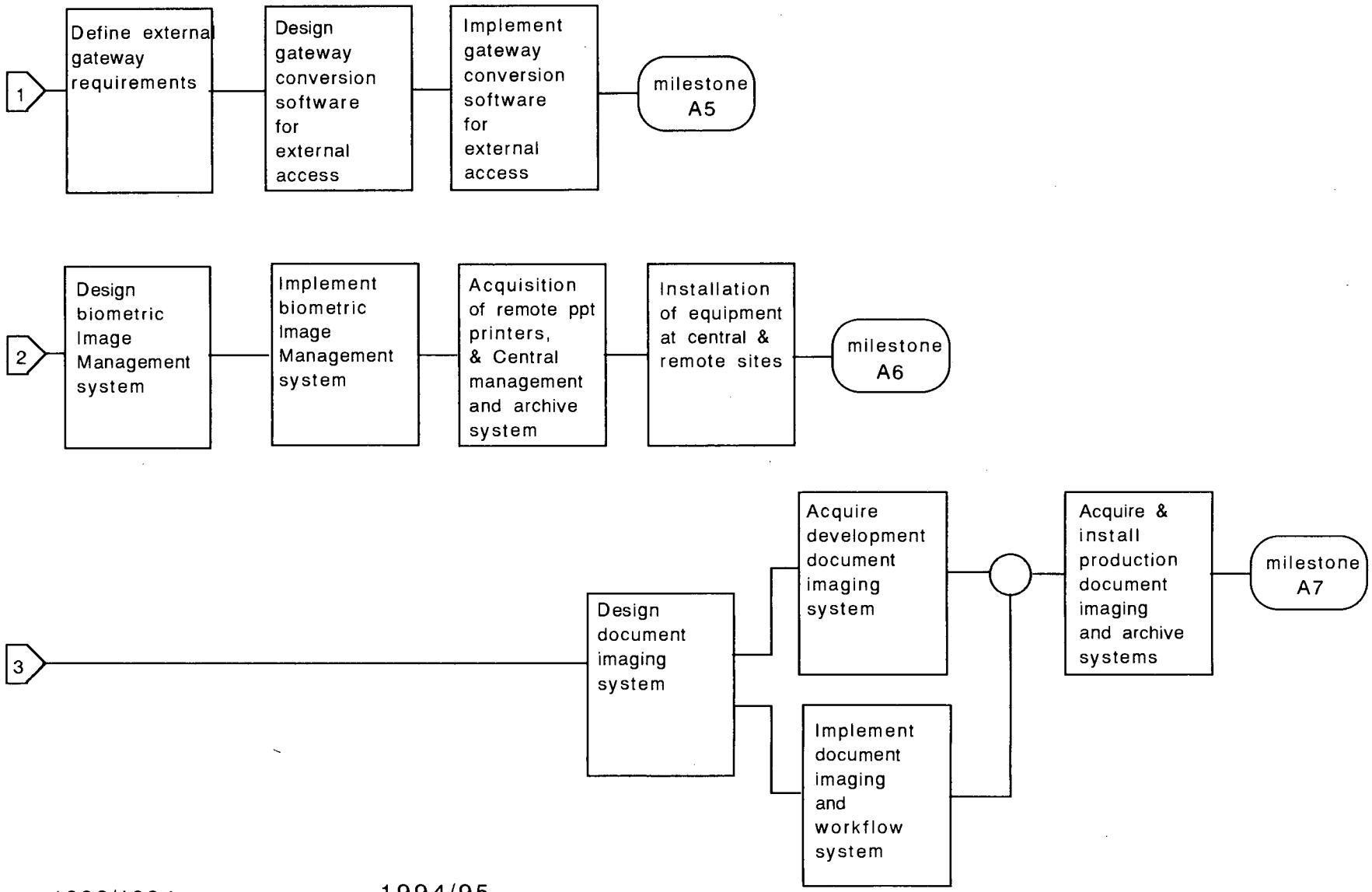
- Electronic archiving of imaged documents will be required in conjunction with its use in passport application processing



1991/1992 | 1992/1993 | 1993/1994 ...

STRATEGY A part 1

Figure 9 - 1



STRATEGY A part 2

Figure 9 - 2

Strategy A Milestones

Refer to Figures 9-1 and 9-2 for the Strategy A planning chart.

1992	A1	Complete architecture & requirements definitions.
1992/93	A2	Install initial image capture system; begin building image data base.
1993/94	A3	On-Line Guarantor data base to be set up with both local and remote access from PPO lacations.
	A4	Expanded, on-line Master Index and PCL data bases, or their replacements, to be made accessible locally and remotely (including missions abroad).
1994/95	A5	On-line access to Federal and Provincial data bases for vital statistics checks and other security checks.
1995	A6	Production of passport using imaged biometrics and electronic archiving of images.
1995 +	A7	Processing of applications using document imaging and "workflow" systems; electronic archiving of documents.

Strategy A Tasks

The following general tasks have been identified which would be required in order to implement the above technical directions:

1. Architectural study and requirements definition. This task is essential to understand the basic topology and computer systems and network structures that will form the foundation of the future implementation. It establishes an important context for future systems planning and specification.

2. Define desired Canadian passport directions and requirements for 5-10 years, updateable every 2 years. This task should be carried out at a senior planning level, and should ideally involve other groups and departments such as Immigration.

3. Research available biometric capture facilities and select one for collection and simple non-operational retrieval of digitized images in the near future. This action will permit the main data files to be totally upgraded with basic biometrics in a 4-5 year period, even though a full operational system is in the future.

4. Central file servers to be established, with SQL-like client-server software to be chosen.

5. Guarantor data base to be designed and implemented, within the new architecture.

6. New PCL and Master Index data bases to be designed and implemented, within the new architecture.

7. Acquisition of equipment to expand network to remote sites.

8. Gateway conversion software to be designed and implemented for access to/by Federal/Provincial agencies.

9. Research and define requirements for biometric imaging and document imaging. This effort will take plac approximately one year after biometric data collection had begun, and will benefit from the experiences to date with this technology. The early system will also be a good demonstration tool to explain the program to counterpart operations and to other government managers.

10. Develop or acquire passport production systems for biometric imaging and passport printing.

11. Acquire archiving system for biometric images.

12. Develop or acquire document imaging and workflow system.

13. Acquire or expand archiving system for document images.

12.1.2 Strategy B

Strategy B assumes an evolutionary path. It is assumed that integration of various functions will be left untill later in the project and that communications will initially be similar to the current system (batch transmissions overnight within Canada, and physical transportation of disks for foreign missions). The Master Index remains centralized. The focus is on separate "stand alone" MRP systems with enhanced PCL checking and local guarantor checking in the short to medium term. This strategy assumes the technical goals are:

- Maintain MRP systems as key to passport production with expanded PCL checking and local guarantor checking for the short to medium term.

- Utilize biometric data for production of passports by 1994/1995.

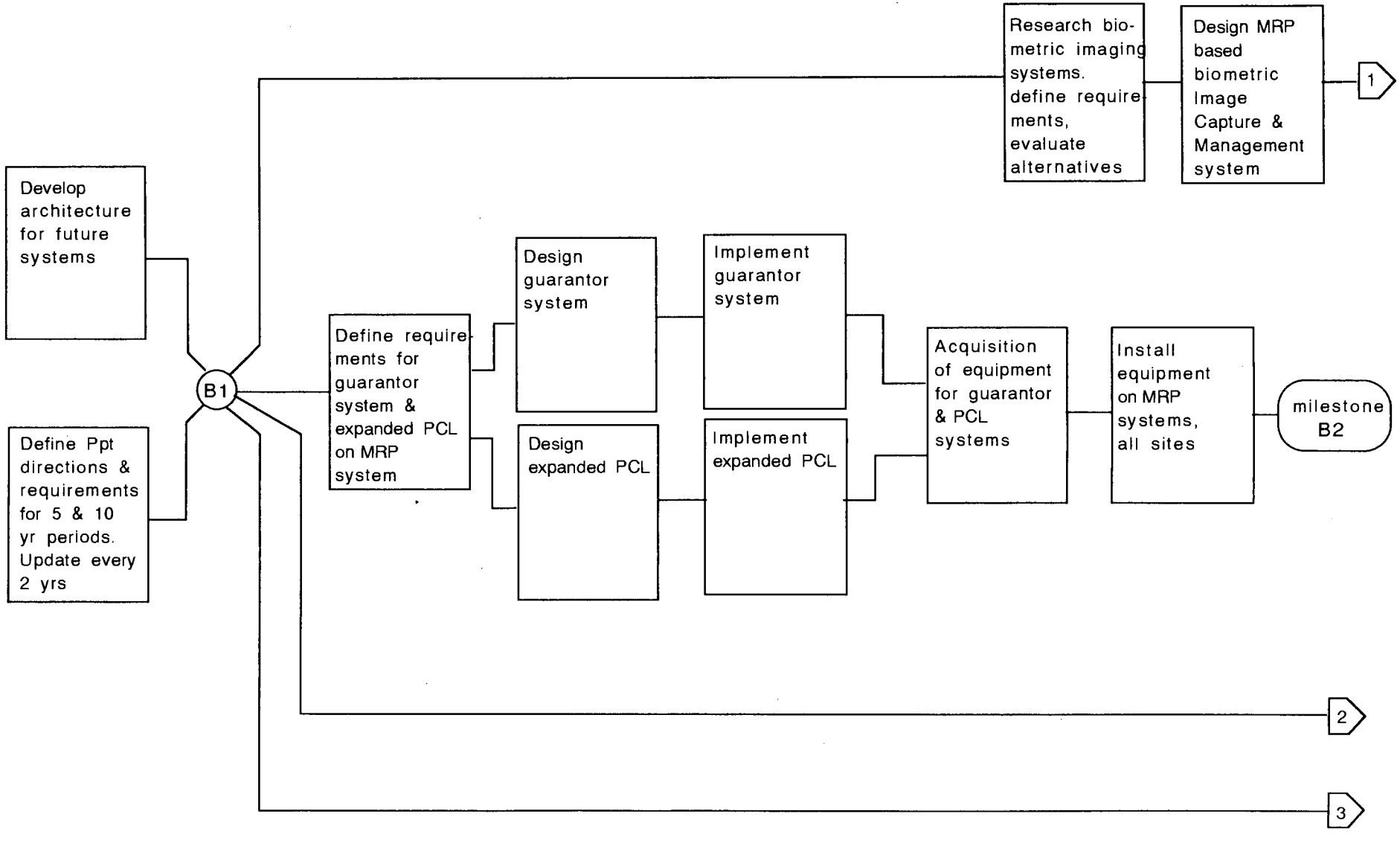
- Electronic archiving of biometric data will be required in conjunction with use in passport production.

- In the medium to long term, provide on-line access of data bases from regions and missions and transmission of MRP data to update the Master Index.

- Provide access to external data bases (Federal and Provincial vital statistics, police, immigration, etc.) and controlled access to Passport Office data bases for other departments and agencies.

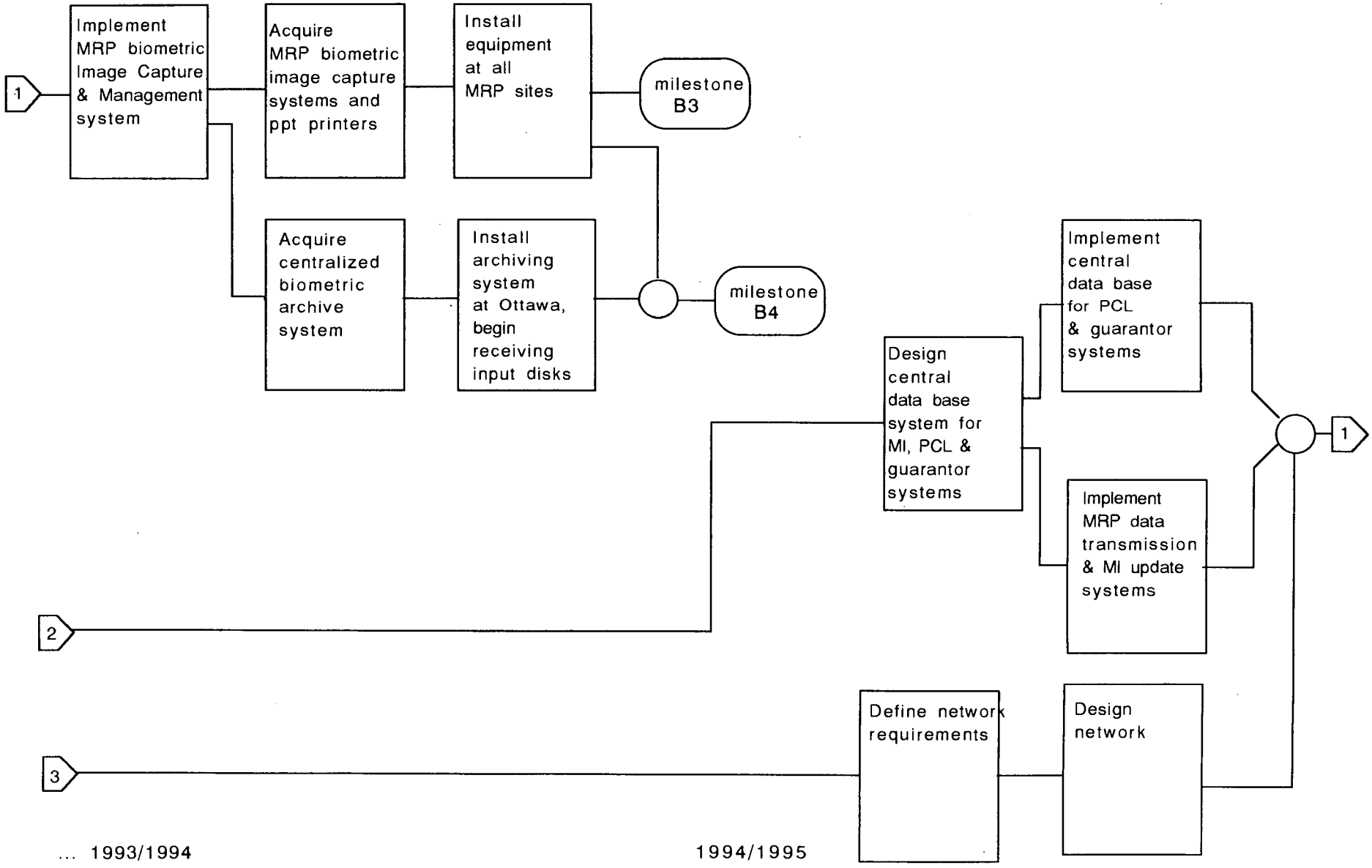
- Imaging of documents and electronic "workflow", as distinct from biometrics capture, is treated as a long range goal.

- Electronic archiving of imaged documents will be required in conjunction with its use in passport application processing.



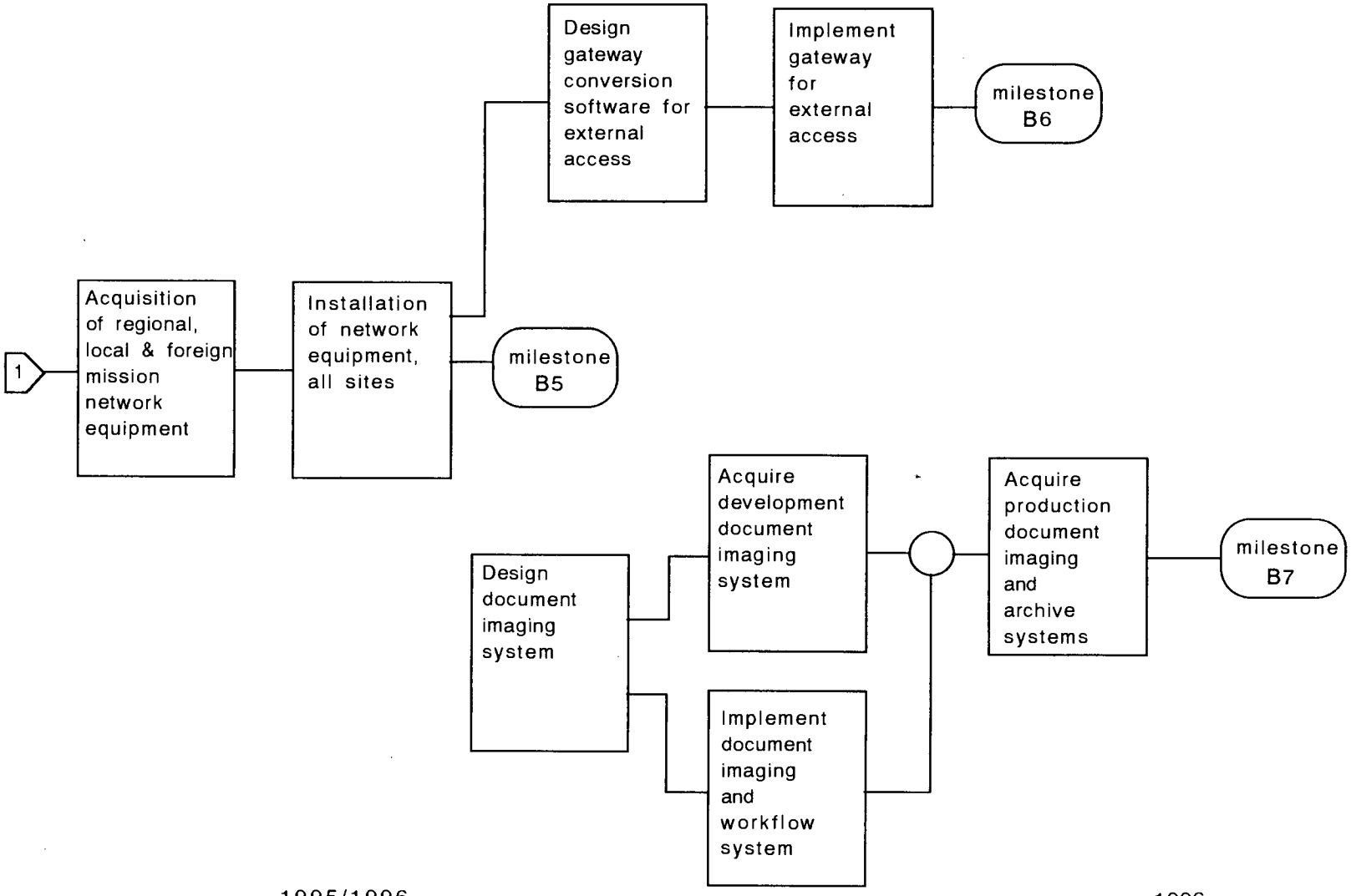
STRATEGY B part 1

Figure 10 - 1



STRATEGY B part 2

Figure 10 - 2



STRATEGY B part 3

Figure 10 - 3

Strategy B Milestones.

Refer to Figures 10-1, 10-2, and 10-3 for the Strategy B planning chart.

1992	B1	Complete architecture & requirements definitions. This task is common with Strategy A.
1993/94	B2	Add guarantor data bases to MRP systems and expand PCL data bases.
1994/95	B3	Production of passport using imaged biometrics.
	B4	Archiving of imaged passport biometrics via manually transported data (on disk).
1995/96	B5	Centralize PCL & guarantor data bases - on-line access for all users; update Master Index from on-line MRP systems.
	B6	On-line access to Federal/Provincial data bases for vital statistics checks and other security checks.
1996 +	B7	Processing of applications using document imaging and workflow systems, electronic archiving of documents.

Strategy B Tasks

The following general tasks have been identified on the charts which would be required in order to implement the above technical directions. Note that no early capture of biometrics data is assumed here.

1. Upgrade current mini computer, integrate more closely with Ottawa LAN as file server.

2. Add guarantor data base as regional system (similar to PCL operation).

3. Expand information on PCL and make case information available for security.

4. Integrate MRP systems with LANs in Ottawa & regional offices, capture information on documents presented with applications.

5. Upgrade MRP systems with biometric image capability, upgrade mini-computer with archive capability.

6. Integrate remote MRP's via the WAN. On-line access to centralized guarantor, PCL, MI data bases for all users.

7. Add document image processing and workflow system.

8. Acquire or expand archiving system for document images.

12.1.3 Capital Costs

Strategy A is the recommended strategy for the Passport Office. Its objectives are essentially the same as those for Strategy B, but the action plan makes it more apparent to all concerned that the PPO has decided on its goals and is planning to achieve them in a timely manner. In addition, given the pace of change both in technology as well as in world politics, the PPO will be able to meet anticipated needs and provide additional services sooner with Strategy A. Also, cash flow may be greater with Strategy A, but only by concentrating expenditures in 4 years vs. 5-6 years. Overall costs of Strategy B may in fact be higher overall, due to the need to prolong and support present technologies while implementing imaging alternatives.

It was beyond the time availability of this study to cost out the complete operational costs for the alternatives derived. Costs of computer systems to implement the recommended new approaches have been provided in section 11.2, and suggested scheduling and milestone charts have been presented earlier in this section. These have been combined here in Chart 1 on the next page, which shows how capital expenditure cash flows may occur over the next several years. Strategy A is used as the basis for this chart, with some costs extended to year 5 to realistically include some installations overseas and the like.

The material in the chart should be treated as suggestive only, for two reasons. Firstly, in this complex area, no precise attempt could be made to configure and size a true system implementation to meet the needs of the PPO. Although the estimates provided are carefully developed, there is still the possibility of error which is particularly dangerous if on the low side. This concern may be balanced, however, by the fact that since imaging is an emerging technology destined to be a very significant one for the 90's, it will also experience dramatic price reductions and competitive availability from major suppliers. As a result, the costs shown may indeed be conservative.

PPO capital equip

	A	B	C	D	E	F	G	H	I	J	K
1	ITEM		YR 1		YR 2		YR 3		YR 4		YR 5
2		QTY	$ 000s	QTY	$ 000s	QTY	$ 000s	QTY	$ 000s	QTY	$ 000s
3											
4	SMALL OFFICE @ $37.5K		$0.000	2	$75.000	4	$150.000	4	$150.000	2	$75.000
5	(2-5 PYs, 2 workstations)										
6											
7	MEDIUM OFFICE @ $43.5K		$0.000	2	$87.000	4	$174.000	4	$174.000	1	$43.500
8	(6-12 PYs, 4 workstations)										
9											
10	LARGE OFFICE @ $166K		$0.000	1	$166.000	2	$332.000	2	$332.000		$0.000
11	(20-25 PYs, 19 wkstns)										
12											
13	MISSION ABROAD @ $37.5K		$0.000		$0.000	2	$75.000	4	$150.000	4	$150.000
14	(1-3 PYs, 2 workstations)										
15											
16	HEADQUARTERS $881.5K tot		$388.000		$493.500						
17											
18											
19											
20	TOTAL YEARLY COST		$388.000		$821.500		$731.000		$806.000		$268.500
21											
22											$3,015.000
23											
24											

13. The Informatics Organization

As part of this study, the current Management Services organization was reviewed with the intent of determining where suggestions could be made to assist the Passport Office in preparing for informatics changes, particularly those envisioned in this report. The results are presented in this section as functional reommendations rather than in the form of a detailed organization chart, in order to permit the PPO to examine further and make its own decisions regarding any appropriate organizational changes.

13.1 Current Orientation

The present operation of the PPO MS EDP organization seems to be effective and traditional for the kinds of computer processing systems managed. Major organizational elements include the following:

1. Application development and maintenance. This is accomodated by a small number of analysts and programmers, with most design, development and support carried out in-house.

2. Application and system operations. These computer servics are carried out by a separate section of operators, headed by the manager in charge of application development. A second aspect of this service, namely quality control of data and output, is organized as a separate group within MS.

3. Technical support. Not identified as a separate category, it is likely provided by the applications development group.

4. Technical R & D. This is provided by a separate position and individual within the MS Diretorate.

5. O & M. Provided by a separate unit within MS.

13.2 Future Roles and Organizational Structures.

Any new strategic directions taken by the PPO, such as those suggested as a result of this study, must of necssity involve a similar change in the organization and operation of the informatics group. The suggestions below are predicated on many of the elements of the basic strategic directions presented elsewhere in this report, and are also focused on these essential principles:

- Organizational delineations must correspond to and permit focus on the objectives and mandate of the PPO, of which informatics is a fundamental strategic component.

- Organizational elements should avoid overlapping duties wherever possible. Each major element must be clear as to its own area of responsibility.

- Correspondingly, each major element must, to the greatest extent possible, be budgetable for $ and PY's as isolated elements of the PPO budget and plan. Costs (and $ returns) of distinct operational programs and services must be discernable, measurable, and able to be rationalized. This is essential to carry out the role of a Special Operating Agency.

As a starting point, it is recommended that the Management Services organization re-affirm for itself that **it is not simply an efficient computer organization, but a specialized provider of a computerized infrastructure of fundamental strategic importance to the PPO and its mandate**. The range of services can be expected to expand in the 90's, as explained in this report, and so this Management Services role will become of increasing significance as more and more of PPO operations and special services are linked to and dependent upon the quality and richness of the informatics informatics base within the PPO.

As a result of the above statement, it is recommended that the PPO examine its organization for informatics with the following focus:

(a) Product or application management. The PPO should identify its current and potential services/products, particularly those resulting from its strategic plans for the future, and organize informatics elements to focus on each one. For example, it might be reasonable to give individuals the responsibility for one or more services, products, or technical areas, and empower that individual to budget and manage the informatics development and support programs (not the actual design and programming) for those elements.

Some distinct elements might be passport production, on-line data access, on-line passport authentication, biometrics capture systems, and document management systems. Another might be data resource management for the new data bases with biometrics envisioned for the future.

This "product management" approach is very useful and manageable, particularly since it permits focus on what is or should be delivered, not the programming or application maintenance to make it so. The next point should clarify this comment.

(b) Application development and maintenance. All application development, and possibly application maintenance, should be considered for outside contracting. The PPO does not have the personnel resources to accomodate all of the systems changes envisioned, and should recognize these as temporary rather than permanent tasks. The Management Services group should not see itself as being in the computer software development business, but rather should husband its technical resources for internal high level system design, technical liaison, and external contract management needs that the PPO will experience.

This approach will again serve to:

- o clearly identify the costs of each new system initiative and its maintenance costs;

- o Clearly identify the cost of internal contract and system management cost;

- o Permit the PPO and its internal staff to concentrate on its true mandate, the provision of specialized services and the proper planning thereto.

(c) Technical support services. This role should be primarily focused on computer system and communications network management, and be identified as an internal service with a separate and identifiable cost. No application development or maintenance role is assigned.

(d) Technical R & D. This role may be considered another internal service to the product managers.

(e) O & M. Again, this unit is in effect an internal consulting resource to the product managers and others.

(f) Quality control. A separate function should continue, independent of the product management area, to support quality assurance and data integrity requirements.

The above structure will aid the PPO in rationalizing and planning all of its operations involving informatics in a very productive manner. In fact, for better program management, all such rationalized activities might be treated for budget purposes as if they were contracts. This implies defining the following attributes for each:

- specific terms and deliverables;
- expected performance based on measurables;
- costs, in terms of $ and PY counts;
- conditions that may vary results;
- expected returns, if appropriate.

The intent of the above is not to turn the PPO into a stringent business operation, but rather in a constructive manner give to each responsible employee and officer a set of understandable responsibilities, particularly related to the products and services of the organization. Any technological advances implemented by the PPO, like in any other organization with a similar mandate, are clearly better managed by individuals with clear responsibilities, not by working groups with responsibility sharing and overlapping duties.

The reasons for putting these recommendations forward is again to reinforce the true mandate of the PPO, which is not computer services per se, but is closely tied and dependent on modern informatics technology. The PPO should therefore consider the organization of its informatics functions along the lines of its mandate, where product management is more or less a "line" task, and where systems development contract support, technical services, etc. are "staff" services. Each is clear as to role, and therefore can be costed and budgeted, with these costs and budgets forming part

of the business plan for each major product or service thrust. Specific systems development projects should be contracted out where reasonable, since it is not the business of the PPO to actually program applications. Such an arrangement, in total, can have a considerable motivating influence on PPO staff, and can aid the PPO considerably in planning for its evolution over the next decade.

APPENDIX A

Current Systems

APPENDIX A. Current Systems

A.1 Administration

A limited number of administrative personnel are equipped with PCs. This is increasing. Typically, PCs are equipped with:

- "Lotus 1-2-3" for spreadsheet analysis
- "Word Perfect" or "Word Perfect Office" for word processing
- "Q&A" for non-relational database operation
- "AMAX/TAPS/TIPS" for asset management, procurement and inventory (not yet in use)

In addition, access to systems provided by other departments includes:

- "OLPAY" for on-line pay
- "FINEX"

In most instances the PCs are operated as stand-alone devices, not connected to each other or to a central database, although plans are underway to provide more inter connection via a Local Area Network (LAN).

Requirements for administrative functions centre around the need to have

- ready access to information
- quality (accurate) information
- transportability of information between applications.

Provision of these functions would eliminate much manual work and duplication of data entry; accuracy of information would be increased; and sharing of information resources between groups would be facilitated. In addition, it was noted that basic office automation functions such as E-Mail and a forms management system are currently lacking.

In addition, communications with data bases and services outside of the department are required for effective management of the Passport Office as a truly independent Special Operating Agency:

- FINCON, to allow complete integration of all financial systems and full management control of financial systems

- Grievance System, (when available)

- OLIS (Official Languages Information System), database of positions and language requirements

- PICS (Position Information Control System)

It is noted that some of these systems (e.g. FINCON) are only available to those organizations having Ministerial status. Yet as an SOA, the Passport Office is expected to operate as a "free standing" agency. (Access to OLIS as an organization separate from External Affairs is currently being negotiated.)

A.2 Passport Production System

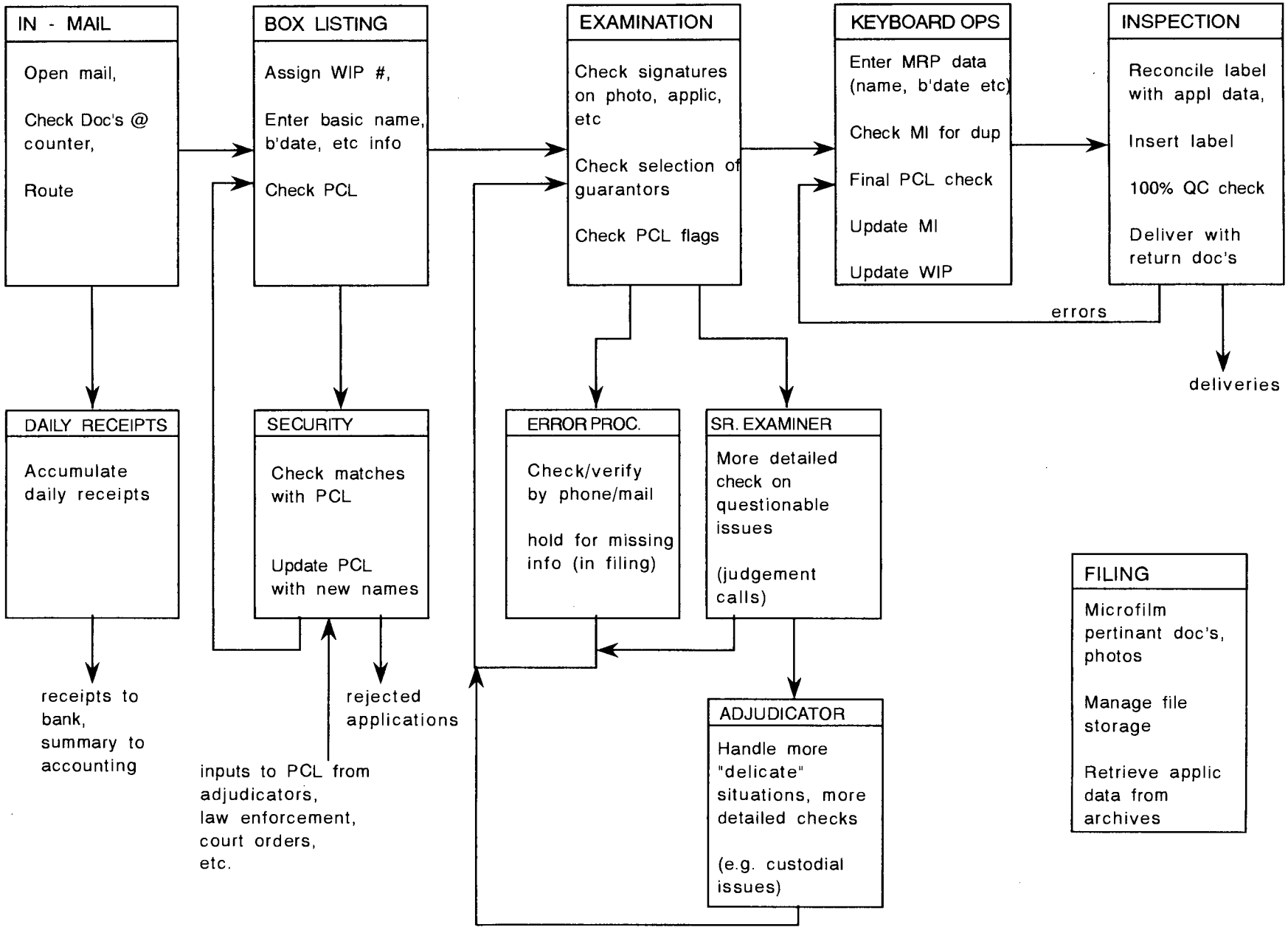
Readers should refer to the work flow diagrams in figures A1 and A2 to assist in reviewing the current PPO passport issue process. An analysis of these procedures was carried out during the study as a means of understanding any current constraints and determining how appropriate evolution might occur.

A.2.1 Headquarters Production System

The following steps are generally descriptive of the issuing procedures for regular passports. Special and diplomatic passports are processed by the same system after being initiated by appropriate documentation from the department concerned. Certificates of Identity and Refugee Travel Documents are processed by a different system (described below) although certain steps in the regular flow are utilized when appropriate (e.g. Keyboard Ops and Inspection). PYs utilized are indicated in parenthesis for each function.

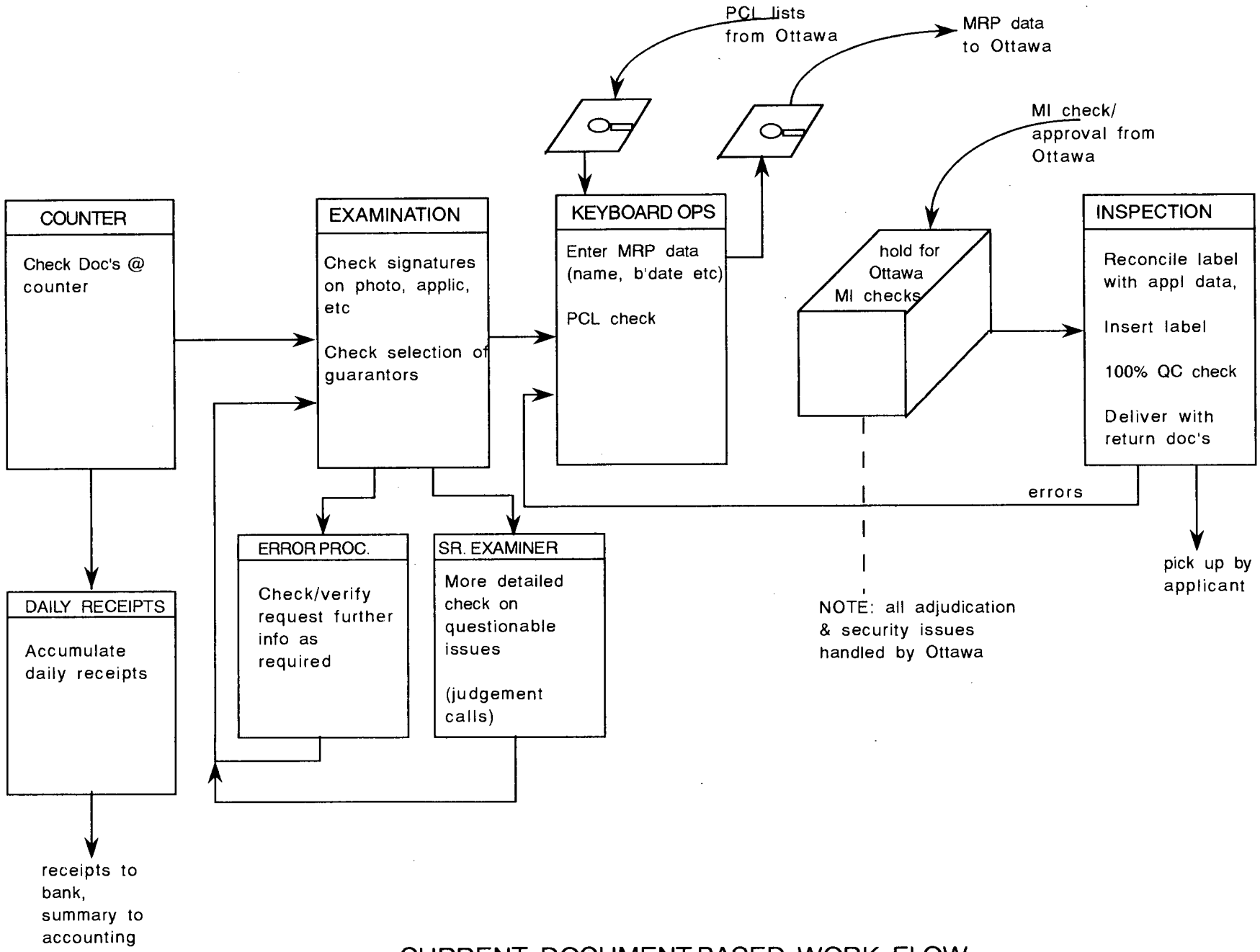
In Mail

Incoming applications are received through three sources: House of Commons, postal service, and walk-in clients. The envelopes are opened and routed to the appropriate destination (e.g. correspondence to section currently handling application, new applications to Box Listing, etc.). Receipts are routed to a collection area where they are totalled on a daily basis. Any applications received at the counter are immediately checked for presence of all applicable documentation and are immediately rejected if not complete.



CURRENT DOCUMENT-BASED WORK FLOW

Figure A 1



CURRENT DOCUMENT-BASED WORK FLOW
- REGIONAL AND LOCAL OFFICES

Figure A 2

Box Listing (11 PYs including In Mail)

Each application is assigned a W.I.P. (Work In Process) file number for future use in tracking the status and location of the application. Basic applicant information (name, birth date, place of birth) is entered into the W.I.P. file and is checked against the P.C.L. (Passport Control List) file. Any matches with the P.C.L. are flagged and the applications are routed to the Security section. Applications that have not been matched on the P.C.L. and any flagged applications returned from Security as OK are forwarded to Examination and W.I.P. is updated to reflect the new status.

Security (6 PYs)

P.C.L. matches are checked further to determine if the match is correct (incorrect matches are possible due to similar names or other such similarities in information). Applications that are OK are marked as OK and returned to Box Listing for continued processing (security may instruct Examination regarding any action deemed necessary). For applications which Security determines should be rejected the applicant is notified and the documentation is forwarded to the security file.

Security also updates the P.C.L. from information received from various sources (police, External Affairs, other departments, court orders, etc.) This may include adding notational information to entries in the list, adding new names to the list, or deleting names.

Examination (26.6 PYs)

Checks are performed on signatures on photographs, application forms, etc. Some guarantor names are checked on membership lists. All applications with P.C.L. flags are checked to ensure that they have successfully passed Security. Xerographic copies are made of identification documents and any other pertinent

documentation submitted with the application.

Any applications with missing documentation, incomplete forms, or other errors are checked and/or verified by phone or by mail. If necessary, applications are held until missing information is supplied.

Any questionable applications are forwarded to a Senior Examiner for further checking. Seniorr Examiners may make judgement calls or use their discretion in approving applications, or may forward more sensitive ones to Adjudicators for further attention.

Adjudicators handle more "delicate" cases (such as those where there might be a question of child custody) and eventually approve or reject the application.

Applications that are routed through error processing, Sr. Examiners or Adjudicators and are eventually approved are returned to Examination for continued processing. After Examination is complete, applications are forwarded to Keyboard Ops.

Keyboard Ops (11.5 PYs)

All passport data is entered onto the M.R.P. (Machine Readable Passport) system and is stored on a floppy disk. (Note that data is NOT taken from the W.I.P. system - it is manually re-entered.) The W.I.P. file is updated with new location/status information. The Master Index is checked for duplicate passport issues and other inconsistencies. If no alerts are detected, the Master Index is updated with the new passport information. A final P.C.L. check is performed here (to catch errors in data that may have been mistyped in earlier stages, or to catch errors in regional or mission issued passports - see following para.) P.C.L. alerts are checked to ensure that the application has been stamped as approved, if not, the file is referred back to Security or Adjudication (depending on the type of alert). Master Index alerts are first checked by an analyst to determine if it is a true duplication - duplicates are re-routed to Security. If no alerts were

detected, the passport label page is printed and the file is forwarded to Passport Inspection.

Regional inputs of M.R.P. are received nightly via communication links. Final checking of P.C.L. and Master Index are done at this point and Regions are immediately notified of any checks. (Regions hold the passport until OK is received.)

Inputs from Posts abroad are received and processed by Keyboard Ops. Automated Posts submit M.R.P. files on floppy disks on a weekly basis. Non-automated Posts submit hardcopy documentation which is then entered on the system by Keyboard Ops. P.C.L. & Master Index checks are done and if alerts are found, the matter is referred to Security (note that in these cases, the passport will already have been issued).

Certificates of Identity and Refugee Travel Documents are also processed at this stage. These are similar to passports in most respects but include observation notes limiting validity to particular countries. They also have different expiration dates which must be entered by the operator.

Passport Inspection (19.8 PYs)

Reconciliation of evidence of citizenship, application form, etc. and the printed i.d. label is performed to ensure that no errors are entered onto the passport label (labels in error are returned to Keyboard Ops for correction and further P.C.L. and Master Index checks). Labels are inserted into passport books and a Q.C. (Quality Control) reading of every passport is done to ensure machine readability. The completed passport and identification documentation submitted with the application are forwarded to the applicant.

Microfilming (12.6 PYs)

Application forms, photographs and pertinent supporting documentation are permanently stored on microfilm and paper documentation is destroyed. It is reported that an average of 2.5 images are microfilmed for each file (front of application plus front of photo = 1 image; back of application plus back of photo = 1 image; miscellaneous documentation on decisions or explaining discrepancies account for .5 image per application). Examiners, adjudicators, and security personnel indicate manually which documents should be retained (other than the application form and photograph). Personnel manually examine each file as they process it for microfilming to determine which documents have been flagged for recording.

Personnel are also responsible for retrieving files from microfilm for use by security, foreign posts, etc. Retrievals are requested at a rate of 2900/month.

Microfiche of Master Index records are produced each year by MIS.

File Storage (15.5 PY's)

Active files that are in production are stored in production areas. Active files that are awaiting correspondence or other action in Ottawa are stored in "pending" files, managed by File Storage personnel; completed files from all regions and posts are forwarded to Ottawa for storage as "dormant" files awaiting microfilming by File Storage personnel. "Dormant" files represent a 3 to 6 month backlog for Canadian passports, and 6 to 9 month backlog for foreign post-issued passports.

Typical retrieval times range from 15 minutes to 2 hours for specified records, and 2 to 4 hours if research is required.

A total of 625 square feet of space is required for file storage.

A.2.2 Certificate of Identity and Refugee Travel Documents

Because of differences in content on application forms and different procedural requirements in checking applications, these documents are handled in a somewhat different manner than the passports. A box listing and WIP process including a PCL check is followed, although by C of I personnel, and a separate storage area for applications is maintained. All applications are checked with CEIC to determine their validity and to verify the type of document to be produced (C of I or RTD). The CEIC check typically takes 4 weeks. Then checks are performed to ensure that no deportation orders etc are outstanding, and guarantor checks are done on a sampling of applications (it is noted that current checking is less than the stated objective due to a large backlog). Any adjudication is done by C of I personnel. After completion of all checks, these applications rejoin the normal passport processing flow at the Keyboard operation stage.

It is noted that typical C of I and RTD files are much larger than passport files because of the need for additional documentation and for a significantly larger volume of correspondence with applicants who may not have a complete understanding of the English or French languages. The entire process is much more paper intensive than the regular passport flow and is much more likely to require special attention by C of I personnel - it is estimated that only 3 out of 12 applications are processed without requiring information in addition to that which was submitted originally.

Because these documents are issued for a limited period of time (1 or 2 years), renewals are frequently requested. A large file storage area (approximately 400 square feet) is maintained solely for keeping the most recent 2 years of applications.

A.2.3 Regional Production Systems

Regional production flows are similar in nature to that described above for headquarters. The main differences are:

- Lack of Box Listing step and W.I.P. files. It is assumed that since most traffic is "walk-in", that the W.I.P. step is unnecessary.

- P.C.L. checking is done on a slightly abbreviated list, containing name data but minimal additional information.

- Keyboard Ops cannot check the Master Index for duplication etc., therefore all passports are held until M.R.P. data has been transmitted to Ottawa and checked against the Master Index (and P.C.L. again).

- Any PCL or MI alarms cause the application to be forwarded to Security in Ottawa for rectification

A.2.4 Foreign Post Production Systems

Production flows at the posts are somewhat simplified to those described above.

- P.C.L. checking is done on a yet more abbreviated name list (automatically on posts equipped with an M.R.P. system, manually from a hardcopy list in un-automated posts).

- Replacement passports are issued with a maximum validity of 6 months.

- M.R.P. files are forwarded to Ottawa periodically by automated posts

(weekly or bi-weekly) on floppy disk. Manual posts forward hardcopy information.

A.3 Limitations and Restrictions of Current System

A.3.1 Technology related issues

The current system suffers from a general lack of capability for distributing information to the remote locations where it is required for timely and appropriate decisions.

- PCL lists are distributed in a variety of ways with several levels of abbreviation, which hinder decision making when needed supplemental information is not available - unnecessary delays occur while headquarters is consulted.

  The time delays in distributing the PCL to foreign posts, when added to delays in returning data on issued passports to headquarters, can result in a gap of several weeks in total before a PCL check is done on an up-to-date list.

- Master Index checks at foreign posts are done on aged data, due to delays of several weeks in periodic updates for these posts. This is compounded in the final checking process at headquarters by equivalent delays in return of data on passports issued.

- There are no means to quickly transmit biometric data - even a photograph - to remote locations when a check is needed. Photographic images are stored on microfilm and require significant time and manpower to retrieve and no electronic means exist to transmit images.

- The quality of image reproduced from microfilm is sometimes insufficient for identification purposes. The Crown has lost criminal cases on the grounds that reproductions were not sufficiently clear.

- Because of the large volume of paper in each C of I or RTD file, errors in microfilming frequently occur. Documents are sometimes missed which should be copied.

- There is no data base of guarantors that can be easily checked, thus guarantor checking has been done on an exception basis and on a sample basis. There is no on-line data base of questionable guarantors.

  Some regional/local offices maintain their own card indices of guarantor signatures, some do not, thus checking is inconsistent between offices. Also, the workload involved in maintaining such an index is significant although deemed beneficial by those offices that do maintain them.

- There is no means to connect to any Provincial systems for birth/death records that might aid in identification checks.

- It has been reported that during periods of unavailability on the computer system, PCL and Master Index checks have been omitted from the procedure in issuing passports on an "urgent" basis.

- Limited statistical information is available from the computer system, and is primarily production oriented. It is not feasible to perform analysis of passports issued for the purpose of detecting questionable practises.

- Although generally an efficient manual operation, duplication of some operations (e.g. PCL check) does occur, in apparent attempt to prevent omission due to differences in procedure between offices as data is forwarded to headquarters.

- MRP computers (PC/XTs) are limited in capability, and cannot accomodate disk sizes required for more complete PCL lists.

- There is no integration of the central computer system with any PCs in administrative functions. Any analysis of data requires manual transposition of data between systems for analysis on PCs.

The CUPID (Computer Utilized Passport Information Database) system runs on a Honeywell "Ultimate" computer and provides support for the WIP system, the PCL database and statistical gathering for production information. The "Ultimate" computer system was installed approximately five years ago, and thus does not have many of the capabilities that will be required of it to implement some of the new technologies that are likely to be needed in the future. (It is noted that replacement of this system is already being planned.) Its configuration includes:

Hardware:

- 6800 CPU
- 2 M Bytes of main memory
- 2 G Bytes of disk memory
- 96 I/O ports
  - 8 for remote communications
  - approx 80 "dumb" asynchronous terminals - Wyse 50
  - 10 PCs emulating Wyse 50 terminals
- 1 Centronics printer
- 1 low speed GE printer
- 1600/6250 bpi magnetic tape drive

Software:

- "Ultimate" operating system software with
  - utilities
  - data base management
  - BASIC compiler
- "Ulti-Calc" spreadsheet
- "Ulti-Plot" plotting package

A small LAN has been installed to connect approximately 35 PCs withing headquarters. This is being expanded and will soon have 70 PCs on it. The software available on the LAN includes:

- Netware 3.1.1
- Certus (management & virus checking)
- Lotus 1-2-3
- dBase 3
- WordPerfect Office
- Q&A 4.0
- DrawPerfect 1.1
- Harvard Graphics
- Viaduct (communications emulation for connection to Ultimate)
- Grammatek 4.
- XTREE Net

The MRP production system is based on a PC/XT (or clone) with MS-DOS software, special utilities written by the Passport Office, daisywheel printers, and "Crosstalk" software for communications. Approximately 40 of these systems are installed in Ottawa, Regional offices and missions.

APPENDIX B

Technologies Investigated

APPENDIX B. Technologies Investigated

This appendix discusses in more detail some of the promising technologies which were investigated during the course of this study. Implications for the PPO are reviewed earlier in the report. Current costs of different units are presented for information purposes.

B.1 Document imaging

B.1.1 Scanners

Scanners are available for both black and white input and colour. With resolution of 300 dpi, excellent reproduction of text, document images, and line drawings is possible (as exemplified by systems from many major manufacturers - Wang, IBM, Sun Microsystems, Kodac, etc.). However, handling of photographic images may be somewhat easier with video camera input and "screen grabbers" since scanned input cannot be viewed until the entire image has been input and adjustments may be required before the final image is captured.

Recent advances in the field of document imaging have resulted in full size document scanners with resolution of 300 dpi costing as little as $2,000.00 to $3,000.00 for black and white units and $3,000.00 to $5,000.00 for colour units.

B.1.2 Video Input

Video input devices are available which use a digital camera (or digitized image from the camera) and a "screen grabber" interface in a PC or workstation. The continuous input from the camera can be viewed on a screen (a separate screen on some systems, or the regular PC console screen if appropriately equipped on other systems). The document being imaged can be manipulated (e.g. to ensure correct orientation or correct sizing) and when the operator is satisfied, the image can be

transferred to computer memory by the "screen grabber". A colour head-and-shoulders image can be compressed to approximately 20K bytes of memory without losing image quality.

Video cameras and screen grabbers are only slightly more expensive than scanners: $5,000.00 to $8,000.00.

B.2 Communications

B.2.1 Local area Network (LAN) equipment

B.2.1.1 Workstations, Servers

These devices have a great range of capability and price, from a small PC in the $2,500.00 to $5,000.00 range; to high power workstations from companies like Sun Microsystems, Appollo, IBM, etc costing $10,000.00 to $100,000.00; and "super minis" or midrange machines such as DEC VAXs, Wang VS8000s, IBM AS/400, etc. costing $50,000.00 to several hundred thousand dollars.

The smaller PC based units are usually limited in function to supporting local processing for single users (e.g. displaying documents, editing text), while midrange or higher power workstations may act as multi-user systems or various types of server (e.g. an OCR scanning function could be run on this type of device). Larger "super minis" or midrange machines are usually limited to acting as file servers for large data bases.

The cost of connecting any of these workstations or servers to a LAN is usually minimal compared to the cost of the computers themselves. A typical interface card will cost $1,000.00 to $2,000.00 to connect to a token ring or Ethernet LAN. FDDI costs are somewhat higher: $5,000.00 to $10,000.00 per connection.

B.2.1.2 Bridges, routers

Bridges and routers are used to connect multiple LANs over local or long distances. While performing similar basic functions, bridges operate at a lower network layer of the OSI model and perform a simple point-to-point (or point-to-multi-point), protocol transparent, transmission service; routers operate at the Network Layer of the OSI model and provide more sophisticated, multi-path routing. For wide area bridging or routing, all of these devices require either dedicated telecommunication lines between them, or connections to X.25 packet networks.[10] [11]

Simple bridges can be purchased for $5,000.00 to $10,000.00 each; more sophisticated routers will cost $15,000.00 to $30,000.00 depending on configuration and capability. Suppliers include: Cisco Systems Inc, Wellfleet Communications Inc, Network Systems Corp , Timeplex Inc. ($8,000.00(Ethernet only) - $29,800(4 Ethernet & 2 FDDI)).

B.2.1.3 Cabling systems

To connect the workstations and servers of any single LAN, it is necessary to have a cabling system in place. Cabling systems are available based on a variety of media: COAX cable (2 types), twisted pair copper wire (shielded and unshielded), fibre-optic cable, and even wireless systems based on various broadcast technologies (spread spectrum, narrow band and infra-red)

In order to optimize and manage cabling systems, a variety of concentrator, hub and distribution systems are available from suppliers such as Cabletron and Synoptics.

---

[10] "LAN Interconnect Using X.25 Network Services", John Barrett, Eberhard Wunderlich, *IEEE Networking*, Vol 5, No 5, September 1991

[11] "LAN Interconnection Across SMDS", George Clapp, *IEEE Networking*, Vol 5, No 5, September 1991

Because each LAN location is subject to differing factors, such as availability of suitable cabling, renovation costs for installing cable runs, length of cable runs, number of workstations, etc., it is virtually impossible to give even a "typical" cabling cost.

B.2.2 Wide Area Network (WAN) equipment

Interfaces to Wide Area Networks are available in a variety of forms depending on the type of WAN and speeds to be supported. For LANs, a separate communication server might be required to interface to an X.25 network or to several high speed T-1 links. One server might be able to handle connections to multiple types of networks. Typical prices for a communication server would be $10,000.00 to $15,000.00. For an individual PC, a simple serial interface is normally included as a basic part of the PC. Modems would also be required for each connection - a dial modem for low speed access (2400 to 9600 bps) would cost $500.00 to $2,500.00 depending on features. Higher speed communication lines (64Kbps and T-1) also require termination equipment similar in function to a modem, but these are usually provided by the telephone company as part of the service (this practise will vary from country to country).

B.2.3 Network Services

Generally, wide area networking costs vary with speed, distance, type of service, and in some cases, proximity to a major telecommunications serving area. Because the topology of any future network is impossible to predict at this time, cost estimates have not been provided.

B.2.3.1 Low speed dialed and leased lines

Relatively low speed (1200 to 9600 bps) communication is easily accomplished by connection to the dial network, at costs identical to those of regular voice calls. Similarly, dedicated lines may be installed between offices to provide a permanent communication facility. Due to the relatively low speeds, these services may be better suited to linking remote offices to regional centres or for emergency back up of other facilities than for use in linking major centres. (Per the example in section 4.2, a 20KByte image that would take 16 to 20 seconds to transmit at 9600 bps would take 130 to 160 seconds at 1200bps.) Also, depending on the volume of use, connection to a packet network may be considered as an alternative to these facilities.

B.2.3.2 Medium and high speed services

56Kbps and 64Kbps digital switched or dedicated services are now available linking most major centres in Canada. As ISDN networks are installed internationally, 64Kbps services will become also available to many foreign posts. Though costing more in absolute dollars than low speed analog lines, the cost per bps of these services can be significantly lower. (Our example 20KByte image used above would require 2.5 to 3 seconds to transmit at these speeds.) It should be noted that typical PC communications interfaces (e.g. "comm ports") may not be able to operate at these speeds - connections to this type of service would probably be from a LAN communication server or "super-mini" computer.

Higher speed services such as "T-1" are also available within major cities and between major centres. These services operate at 1.5 Mega bps within North America and 2 Mega bps in other countries. Services such as this are best suited to linking LANs with high volumes of traffic or strict response time requirements (Our 20KByte example image would require approximately .1 seconds of transmission time at 1.5Mbps).

Typically these services would be used between major centres where traffic volume could justify the costs or within a single city to link LANs in several offices.

B.2.3.3 Packet networks

Public packet networks are available across Canada and around the world in virtually all developed countries and most "developing" countries. Most of these networks provide connections at low and medium speeds (1200 to 64K bps) at relatively low cost compared to dial or dedicated facilities. Most packet networks charge a fixed monthly amount for a physical connection, plus a charge based on volume of use (number of packets, number of logical channels, etc.). This makes them ideal for many applications with light or variable volumes of data. In addition, international gateways exist to allow transfer of data between virtually any combination of endpoints.

In order to connect to a packet network, a computer would have to be equipped with a suitable communications port and software. This could range in price from $2,500.00 for a single line on a PC to $10,000 to $15,000 for a communications server. It is also possible to configure some LAN routers with X.25 ports.

Private packet networks may be built by installing X.25 switching equipment and leasing dedicated telecommunication links between switches. For purposes of the Passport Office, it is probably not economically feasible to implement an entire network dedicated solely to their own use, however, the possibility of connecting foreign posts via External's MITNET in some way should be investigated.

B.2.4 Network Management

Regardless of the network facilities eventually installed, a means to manage the resulting network will be an absolute necessity. Assuming some kind of LAN or WAN is installed in multiple sites, it will be highly desirable to manage the system from a central location in Ottawa, with few or no technical personnel in remote offices. A network management system must be chosen in conjunction with other network facilities in order to ensure that remote equipment is capable of being controlled by the management system. The entire network, including the

management system, must be considered as an intergral system. The network manager must be able to diagnose problems, measure performance and reconfigure various parameters on network equipment, preferably from his office in Ottawa.

The final network management system will depend on the type of network installed, but could cost $50,000 to $100,000.

B.3 Printing technologies

A number of different types of printers are available for printing black and white and colour images. Because of the different technologies used, it is necessary to consider certain disadvantages or concerns related to each type and certain advantages of some types.

- The ease with which the printed image can be removed when using inks that are deposited on the surface of the paper (as opposed to those that are absorbed into the paper). This can be countered with security laminates to protect the image as is currently done with the Canadian passport and with pre-printed patterns on the label, sensitive to removal.

- The difficulty of providing security in reading the machine-readable portion of the page when using standard inks which are infra-red absorbing (rather than infra red reflecting as required by the ICAO standard). This can be countered with special inks in most types of printers, but may require a second pass through a black and white printer.

- The quality of the image will vary directly with the density of the printed dots. The standard low-cost printers typically output at 300 dots per inch (dpi), higher cost printers can be purchased for 400, 600 or even 1200 dpi. While perfectly adequate for typed output and line drawings, 300 dpi is probably not acceptable for good quality image printing with most of the techniques under discussion (except for die sublimation printers).

The types of printers considered in this report include the following:

- Black and white laser printers. These are very inexpensive devices in common use with personal or micro computers and are available from a large number of manufacturers. Typically they print at 300 dpi and cost $2,000.00 to $4,000.00. Higher quality output is available for higher prices (e.g. $5,000.00 to $20,000.00 and up). As noted above, higher density output is required to obtain near photographic quality image.

- Black and white and colour ink-jet printers. These are even less expensive than laser printers, ($1,000.00 to $2,000.00) but suffer the same drawbacks that laser printers have. Most are limited to 300 dpi output.

- Colour laser printers. These devices use similar technology as black & white laser printers, but with three colour inks. The costs range from $5,000.00 and up. These devices suffer the same lack of photographic quality for images as black and white units, and in addition, cannot produce machine readable data lines since they are loaded with three non-black inks. A second pass in another printer would be required to print the MRP portion of the label.

- Die Sublimation colour printers. These devices have a wide range in prices from as low as $6,000.00 for a small format unit (approximately passport size) to as high as $70,000.00 for full page high speed units. The printing technique is slightly different than the other devices described here in that it requires a receptor to be pre-printed on the paper. Because of the die sublimation process, the image is closer to a continuous tone colour photograph than those available from the other techniques. Another benefit of this process is the fact that the die is absorbed to some extent by the paper, making removal of the image very difficult. It is noted that a major operating expense of die sublimation is printer ribbons - current costs can be as high as $1.00 per small format page. The images produced by this technique can be protected by covering with a laminate (albeit a different one than currently used). One drawback of this technique is its inability to produce a machine readable data line - a second

pass with a laser (or other type) printer would be necessary.

- Colour Thermal Transfer (thermal wax colour) printers. These devices use a thermal wax transfer technology to deposit dots of each colour on the surface of the paper from an ink roll. Similarly to colour laser printers, the output is typically 300 dpi quality, but as with other colour printers, true black output is not available, necessitating a second pass to print the MRP zone. Prices are believed to be in the range of $10,000.00 and up.

B.4 Storage devices

The most appropriate type of storage device will depend to some extent on the final application requirements. For example, an archiving function (say a pure "lookup" with no searching), with retrieval time requirements in the order of several hours can function with removable disks stored in an archive room, with operators performing the physical retrieval and mounting of the disks - for faster access, "jukebox" devices are available which can provide access in the order of 15 to 30 seconds. Of course a hierarchy of systems is also possible.

Magnetic disk drives are relatively limited in size, but provide very fast access times - a typical large magnetic disk of 1.3 Giga bytes might cost in the order of $15,000.00 (with controller); optical disks with jukebox options can store up to 100 platters of disk surface (3.2 Giga bytes per platter side) - a small jukebox with capacity for 12 platters of 2 Giga bytes each might cost in the order of $55,000.00; a larger jukebox system with capacity for 100 platters of 3.2 Gigabytes each would be in the $150,000.00 to $200,000.00 range. For use with workstations, very small optical disk systems (1.3 Gigabytes) are available for $12,000.00, including a tape backup unit.

The primary types of large scale data storage devices that should be considered include:

- CD-ROM - optical disks which are pre written with specialized equipment. Typically well suited for distribution of multiple copies of data via physical means, but not very useful for data that changes over time.

- WORM optical disks - optical disks that can only be written once by standard equipment, but can be read many times. Well suited for storage of data that does not change. These disks have good long term reliability (as much as 25 yrs)

- DAT tape - a digital, high density optical tape. Best suited for back-up due to serial nature.

- Re-writable optical disks - similar to WORM disks but can be re-written. Well suited for large volumes of data that do not change rapidly (write times are typically slow). Long term reliability of disks is good (5 years) but not as long as WORM type.