AUDIT OF

DEPARTMENTAL COMPLIANCE TO THE

GOVERNMENT SECURITY POLICY

for the

DEPARTMENT OF THE SOLICITOR GENERAL

Prepared by

progestic
international inc.

222 QUEEN ST
Ottawa, Ontario
K1P 5V9

December 2000

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

The objective of this audit was to verify the Department's compliance to the Government Security Policy (GSP) issued by the Treasury Board Secretariat (TBS). While the Information Technology (IT) security component of the GSP was reviewed, it was not done so in detail as management felt that the audit should concentrate its efforts on the other components of the GSP.

Generally, the Department is well ahead of most federal government departments when it comes to security. Progestic has found that policies exist and have been well implemented. Employees are very security conscience and undergo a detailed security briefing upon their arrival. This helps reduce the risks associated to any observations that we have made.

Over the years, a number of security measures have been implemented which help provide a secure working environment for the employees as well as protect the very sensitive nature of the information that is found within the Department. Our review of the current security measures revealed many positive practices as well as identified some areas that require improvement.

It was found that the management framework surrounding the security function was well established and defined within the Department. However it was found that the workload of the Security Clerk is increasing constantly and should be documented and reviewed with the objective of reducing the tasks or assigning them to another employee. In addition, the current Information Technology Security Officer (ITSO) needs additional training in IT security and consideration should be given to making the position full-time.

Like many other departments, the Year 2000 threat has enabled the Department to update or create a number of important risk management documents such as Threat Risk Assessments (TRAs), Statements of Sensitivity (SOSs), Business Resumption Plans (BRPs), and Disaster Recovery Plans (DRPs).

However, the Department is currently undergoing several changes not the least of which is a refit of its office spaces and much physical movement within the building. As the documents mentioned above do not reflect these changes they need to be reviewed. We recommend that the documents be updated as the move is in progress and reviewed once the move has been completed. We also recommend that a formal process be implemented that will ensure that these important documents be kept up to date on an ongoing basis.

[

16(2)(c)

]

Although personnel security and awareness is generally good within the Department it is being recommended that refresher sessions be given to employees who have been with the Department for a

long period of time (i.e. more than 5 years) in order to inform them of new measures that have been implemented since their employment start date.

[

16(2)(c)

]

Physical security in the Sir Wilfrid Laurier building is generally quite good. Access to the building is controlled by Commissionaires who ensure that all people have an identification card in order to enter the building. Card readers must be activated in order to access office spaces on any of the floors occupied by the Department. [

16(2)(c)

]

The Department extensively uses office automation tools for the creation, storage, and transmittal of information. [

16(2)(c)

] The Systems Division wishes to migrate to a Windows 2000 OS with PKI and strong authentication using smart cards and biometrics. However, funding has not yet been secured for this project even though it has been planned for over one year. We recommend that the Department pursue this plan to add real security to their operating platform.

2. ACKNOWLEDGEMENTS

The Progestic audit team would like to thank employees from the Department for their cooperation and assistance during the conduct of the audit. The team appreciated the time employees made available for interview purposes and the frank answers given to questions posed.

Appendix A contains the list of employees interviewed during the audit.

3. INTRODUCTION

3.1 Background

In 1989, Treasury Board Secretariat (TBS) approved the Government of Canada Security Policy (GSP) and standards. The policy outlines government security requirements and sets organizational and administrative, physical, personnel and information technology security standards. It requires that an independent internal audit function carry out a systematic review and appraisal of all departmental security for purposes of advising management as to the efficiency, economy and effectiveness of internal security measures within the department.

In 1992, TBS approved an amendment to the GSP on the subject of business resumption planning. The amendment requires government institutions to develop, implement and maintain business resumption plans on the basis of threat and risk assessments and in accordance with operational standards. In 1994, a revised version of the policy was also issued to Departments.

In 1994, the Department conducted a comprehensive audit of security based on the 1989 GSP. As there is a requirement to audit the GSP every 5 years, the Department issued an RFP on July 28, 2000 to conduct a new compliance audit to the 1994 GSP. Progestic International Inc. was awarded this contract. The audit was conducted between September and December 2000.

3.2 Description of the Audit Entity

The Department of the Solicitor General (Department) is a small strategic and policy-focused organization that has approximately 220 employees and a budget of approximately $84 million. The Department provides advice and support to the Solicitor General with respect to his responsibility for the provision of direction to four Agencies (i.e. Royal Canadian Mounted Police, Canadian Security Intelligence Service, Correctional Service of Canada, and National Parole Board); enhancement of policy cohesion and coordination within the Ministry of the Solicitor General Portfolio; his accountability to parliament for the Agencies; for his national leadership role in the federal activities in policing, national security, corrections and conditional release; and in his role as the Minister responsible for aboriginal policing.

4. AUDIT OBJECTIVES, SCOPE AND METHODOLOGY

4.1 Audit Objectives

The objectives of the audit were to review and assess the:

- Adequacy and effectiveness of the Department's management control framework in ensuring that the requirements of the GSP are met.
- Extent to which the Department's security policies and procedures are consistent with and comply with the GSP requirements and its communication to staff.
- Efficiency of implementation of both the GSP and the Department's security policies and procedures.
- Extent to which staff are aware of, and have been trained in the GSP requirements.
- Adequacy and effectiveness of the information systems in place to monitor and report upon the attainment of objectives related to the GSP.

4.2 Audit Scope

The scope of the audit covered all departmental activities, controls, mechanisms and systems related to security. The audit focused on issues of compliance to central agency legislation, policies, regulations and guidelines related to security. The audit covered the Department's headquarter's office only, located in the Sir Wilfrid Laurier building in Ottawa.

The audit covered all the elements referred to in the GSP as follows:

- Organizational and Administrative Security;
- Information Technology Security;
- Physical Security; and
- Personnel Security.

The audit of the GSP was conducted during the months of September and October 2000.

4.3 Audit Methodology

The audit was conducted in three phases; namely, preliminary survey, execution, and reporting.

During the preliminary survey phase, we reviewed key security related documents from the Department and conducted interviews with key personnel from the Security administration functions. The resulting report (Preliminary Survey Report) recommended that the execution phase of the audit focus on the security aspects of the following:

- Risk Management;
- Policies, Procedures and Guidelines;

- Budgeting and Planning;
- Security Violations and Breaches;
- Awareness Program and Training;
- Contracting;
- Personnel Security;
- Physical Security (current measures and for the move);
- Records Management;
- Access to Information and Privacy (ATIP);
- Information Technology.

The execution phase included a more thorough review of documents, interviewing more than twenty departmental employees and conducting a number of audit tests. Although employees with specific security functions were interviewed thoroughly, the audit concentrated on interviewing employees from the operational units of the Department so as to assess their awareness of security policies as well as the real implementation of the procedures.

At the end of the execution phase, a point form report was prepared outlining audit observations/findings, suggestions, and recommendations for improving the state of security in the Department.

In the reporting phase, managers involved with security were debriefed during the conduct of the audit to ensure a "no surprise" report of findings, and a full debriefing of the managers was held at the end of the execution phase. This report is the end result of the reporting phase of the audit.

5. OBSERVATIONS AND RECOMMENDATIONS

As mentioned previously, the Department places a high focus on security issues. This can be seen from the physical measures in place as well as the awareness of all staff members. As such, the audit team observed many good practices throughout the Department. Therefore, the following observations contain positive aspects of the security operation at the Department as well as areas that could be improved upon.

5.1 Management Framework

The accountability framework for the security function is well established within the Department. A Departmental Security Officer (DSO) has been appointed to manage the Department's security program. The organization of the security program is well structured and responsibilities for its delivery are mainly split between two Directors:

- The Director, Administration Division is responsible for the personnel, ComSec, records management, physical, and material management security components;
- The Director, Systems Division is responsible for Information Technology (IT) security including the Disaster Recovery Plan;

The management of the Government Security Policy (GSP) program rests with the Director General (DG), Corporate Services and effective communication links exist between the DG and the two Directors mentioned previously. We are satisfied that a security management structure is in place and that it encompasses responsibility for the overall management of the security program.

Much of the implementation of the security policies and procedures rests with the Security Clerk under the Director, Administration. Over the last few years, the number of activities and responsibilities have grown considerably, as has the workload. Some of the tasks are:

- New security clearances for all staff, students, terms employees including fingerprinting and Criminal Name Check;
- Validation of prior security clearance for staff, students, terms and contractors;
- Upgrade to security clearance for current staff;
- Activities related to arrival of employees such as issuance of an electronic physical access control card;
- Activities related to the departure of employees including the transfer of security files to other organizations;
- Roll up of statistics and distribution of security infractions identified during the Commissionaire's floor sweeps;
- Maintenance of a Bring Forward (BF) system to record upcoming events;
- Organizing the security briefing sessions;
- Combination changes to safes, padlocks, and codetronic locks.

Over the last few months Public Key Infrastructure (PKI) was implemented on a small scale and Local Registration Authority (LRA) responsibilities have been given to the Security Clerk. As well, using PKI technology, the clerk now can enter security clearance forms on-line and submit them to the Canadian Security Intelligence Services (CSIS) for a much faster turnaround. However, this has increased the clerk's workload.

Observation 5.1.1

Many of the procedures implemented by the Security Clerk are not documented. [16(2)(c)]

Recommendation 5.1.1

Identify the procedures that need to be documented, prioritize them, and document them according to a reasonable schedule.

Observation 5.1.2

The workload of the Security Clerk is constantly increasing because of new functions and because of sheer volume. This makes it very difficult for the clerk to keep on top of all activities and presents a risk that some activities may fall through the cracks [16(2)(c)]see section 5.8 for more information).

Recommendation 5.1.2

The Department should find ways to shorten some operational activities by eliminating some of the activities while maintaining the same security and risk level. A good example is related to changes in the combinations of safes, padlocks and codetronic locks (please refer to section 5.9 for more on this).

Observation 5.1.3

As mentioned above, the Department has implemented PKI on a very small scale for specific applications and for experimentation. There are currently five employees who have been issued PKI certificates. The LRA is a role that is important in a PKI infrastructure in that this person approves the granting of certificates to individuals. The audit team has found that there is some confusion over the identity of the LRA. Both the Security Clerk and the DSO's administrative assistant believe that they are the LRA. As the use of PKI will grow over the next year, this situation should be clarified.

Recommendation 5.1.3

Clearly define the roles and responsibilities of the LRA function and clearly assign them to identified employees.

Observation 5.1.4

The current Department Information Technology Security Officer (ITSO) has only been in the position for a few short months. The officer does not have much experience in the IT security field and is not scheduled for much formal training. In addition, the officer revealed that he only spends 30% of his time on IT security matters with another 30% being spent as the IT training coordinator and 40% as 2nd level support to the networks. As the Department embarks on Government On-Line (GOL) initiatives and furthers its use of PKI, the ITSO's role will become much more important and demanding.

In order to strengthen the role of the ITSO we recommend that:

Recommendation 5.1.4

The ITSO undergo additional formal training on IT security matters.

Recommendation 5.1.5

Consideration be given to making this a full-time position.

Recommendation 5.1.6

Outside assistance be sought to help with the implementation of PKI in a Windows 2000 environment with smart cards and biometrics.

5.2 Risk Management

As a result of the year 2000 threat, the Department prepared and tested a number of security instruments as follows:

- Statement of Sensitivity (SOS);
- Threat & Risk Assessments (TRAs) for the two Classified Local Area Networks (LANs) as well as for the Unclassified LAN;
- TRA for the Building;
- Business Resumption Plan (BRP) for the Department;
- Disaster Recovery Plan (DRP) for the IT Environment.

Upon reviewing these documents, the audit team has found that they are current, well put together, and comply with the GSP.

Observation 5.2.1

The Department is undergoing several important changes this year. Currently a major "refit" of the Department's physical accommodations is underway, which involves moving organizational entities to new floors over the next few months. [

16(2)(c)

]

Recommendation 5.2.3

To ensure that all SOS, TRA, BRP and DRP documents are kept current over the years, a process needs to be developed that will include updating them when any changes to the affected assets or their environment are affected. This is normally covered through a change management process.

Observation 5.2.2

The last SEIT inspection by the RCMP was done in 1994. This inspection should normally be done every five years. The Department has made many changes to its security since then and is currently in the process of an important refit to the building. This involves moving operational units to different floors and changing the security system. Additionally, the Systems Division is planning to make an important change to the Department's operating platform. It is planning to move to a Windows 2000 server and desktop Operating System (OS) as well as PKI with smart cards and biometrics for strong authentication. All of this should be completed over the next year.

Although the audit team has not identified any major security risks within the Department, it is suggested that the Department request a SEIT inspection once the physical move has been completed and the planned migration to the new IT environment has been implemented.

5.3 Policies, Procedures and Guidelines

Policies are the foundation to any program delivery. The Department has its own security policies (Employee Security and Safety Instructions) that were issued in 1995. This policy and procedures manual is distributed to each new employee during security briefing sessions. In addition, a copy is available on the Department's InfoNet, which also contains direct links to the GSP at TBS. Although employees interviewed during the conduct of the audit indicated that they did not refer to the manual very often, all had a copy of the above manual and were aware that it was also available on the InfoNet. Generally, employees do not refer to the manual because they feel that they are well aware of the policies and procedures.

Observation 5.3.1

The Department's internal security policy and procedures manual has not been updated since 1995. Although it is not referred to that often, it does not reflect any of the changes that have been implemented since then (for example the new employee departure procedures).

Recommendation 5.3.1

The Department should update the manual and ensure that all employees are informed of the new version available.

5.4 Budgeting and Planning

Budgeting and planning for the security function is done as part of the Department's operational plan. There is no specific plan for any aspect of security including the IT security component. As such, there is no specific budget for any of the security functions or initiatives.

Whenever, the Systems Division requires funding for security related initiatives, it must find it in other operational budgets or through TBS submissions (which is the case this year).

Observation 5.4.1

With the advent of the Internet and all its promises and capabilities, security should become a high profile component of any IT plan. It is no longer something that is to be taken lightly or as an afterthought. IT security must be planned well in advance, depending upon the requirements of the organization, as the implementation tools may take time and considerable resources to implement. An example of this is the implementation of PKI. The Systems Division Director has stated his desire to implement PKI throughout the Department. This initiative in itself will help increase the security of the IT infrastructure for storing and communicating documents. However, a PKI deployment is complex, expensive, and lengthy. It must be planned out well.

Recommendation 5.4.1

The Department should articulate specific Security plans that are separate from the operational plans. This will help put more focus on the security function and make its requirements more visible to Senior Management within the Department.

5.5 Security Violations and Breaches

As mentioned earlier, the Department has instilled a strong security awareness program, which has helped to diminish the number of security breaches and violations. Because of the highly sensitive information that it handles, the Department has also implemented a mechanism to reduce security risks after regular working hours. Security guards run regular sweeps of all the floors to verify that:

- All cabinets, safes, and doors are properly locked;
- There are no classified or designated documents left on desks or elsewhere accessible;
- There are no classified documents left in unlocked cabinets.

Any unsecured container that is found is locked and any classified or designated material found is taken away and secured by the guards. A yellow infraction notice is left for the employee and these are tracked on a monthly basis and reported by the DSO to all the Directorates. No specific disciplinary action is taken with an employee receiving an infraction notice. The audit team found that this system is very thorough and is working quite well. Making infractions visible to senior management contributes significantly to their reduction throughout the Department.

Observation 5.5.1

[

]

Recommendation 5.5.1

[

]

Observation 5.5.2

[

]

Recommendation 5.5.2

[

]

Observation 5.5.3

There are a number of logs that are available that show the amount of Internet traffic and the nature of websites visited by employees. [
]There have been a number of cases in the federal government where it was found that employees spent much time visiting sites for non-business purposes and sites that are inappropriate. Whenever these practices are discovered and made public, they can cause an embarrassment to the organization.

Recommendation 5.5.3

[
16(2)(c)
]

5.6 Awareness Program and Training

The Department has implemented a solid awareness program for all new employees (without exception). The program consists of a detailed presentation by the Assistant DSO (ADSO) and the ITSO. The presentation is done on a monthly basis so new employees never have to wait very long before they attend it. In addition, new employees receive a comprehensive security kit that includes all departmental policies. All employees interviewed have stated that the presentation was very good and that it helped them better understand their security awareness and the procedures that must be followed as well as the reasons behind them.

Observation 5.6.1

Many employees have been with the Department for several years and they have not attended an awareness presentation since they started (5, 10, even more years ago). Although their general awareness is good they do not remember all the details and have not been updated of new policies and procedures. For example, most people would not know to whom to report a breach and not many even know who the ITSO is. As well, the procedures for storing electronic classified information is not being well adhered to (see section 5.10 for more information on this subject).

Recommendation 5.6.1

Refresher briefing sessions should be implemented for employees who have been with the Department for more than 5 years. We have found that the highest risk areas in those sections where employees deal with Secret classified information; those who work with Top Secret information are more aware of security issues. It is recommended that the refresher sessions be aimed initially at employees who deal with Secret classified information.

5.7 Contracting

The audit team verified the security measures surrounding the issuing of contracts to the private sector. The process is very thorough and no exceptions are made.

- The manager generally decides on the security level that will be required by the contracting firm. This requirement is appropriately set according to the requirements of the unit, the work that needs to be done, the access to classified information, and the like. Managers are very cautious about setting the right security level.
- The security requirements are included in the Request for Proposals (RFPs) and contracts.
- Persons to be hired through the contracting process must provide their security clearance, which is verified by the Security Clerk with PWGSC Security.
- Only when a security clearance has been verified does the Security Clerk prepare an access card to the building (only when access to the building is required).
- Once a contract has been completed, the Security Clerk revokes the security pass immediately. It is up to the manager to retrieve the physical card.

The audit team found that the security procedures for contracting are adequate for the Department. No improvements are being recommended at this time.

5.8 Personnel Security

5.8.1 Procedures Related to the Arrival of New Employees

When new employees (indeterminate, term, temporary, students, etc.) join the Department, they all follow the same procedures from a security perspective. They are indoctrinated into the Department's culture through consultation with their managers, as well as through the security briefing session mentioned in section 5.6.

As well, a complete security verification is done to ensure that the employee satisfies the security requirements of the position. An employee is not granted a physical access card until his/her security clearance has been verified. Should an employee not have the appropriate clearance level, his/her employment start date may be affected. No access to any secured storage containers is granted until the security clearance has been completed. Additionally, access to the LAN is not given until the physical access card has been obtained.

The audit team has determined that the procedures relating to the arrival of new employees are very thorough and acceptable for the Department.

5.8.2 Departure of Employees

The Department has adopted a formal process when an employee departs. The employee fills out an electronic form which is automatically submitted to all those people responsible for ensuring that items are returned, passwords are cancelled, etc.

Although this process is worthy, the audit team has the following observations and recommendations:

Observation 5.8.1

[

16(2)(c)

]

Recommendation 5.8.1

[

16(2)(c)

]

Observation 5.8.2

[

16(2)(c)

16(2)(c)

]

Recommendation 5.8.2

[

16(2)(c)

]

Observation 5.8.3

[

16(2)(c)

]

Recommendation 5.8.3

[

16(2)(c)

]

5.9 Physical Security

5.9.1 Building Refit

The Department is currently in the midst of a major move within the building that will involve all units. Part of the move was completed recently (the 12th floor tenants were moved to the 9th floor). For an organization like the Department, moving involves a number of complexities because of the high number of security areas.

The Department has been very diligent in seeking help for the design of the new office spaces. The RCMP have been extensively involved in the project as they have overseen the design of the new installation.

The audit team has reviewed the new design and are of the view that all concerns have been addressed adequately. Thus, there are no observations or recommendations on the building refit.

5.9.2 Building/Floor Access

Access to the Sir Wilfrid Laurier building is controlled in a number of ways. First, there are security guards from the Corps of Commissionaires (CoC) who control access to the elevators. They verify that anyone wanting entry to the building have a pass. Visitors must report to the security desk and request a pass and require an escort to the premises. The Commissionaires are very diligent in ensuring that people have a pass that is visible upon their entry.

All of the Department's floors are secured with a pass access security system [16(2)(c)]. The 8th floor houses NSD and IG CSIS. Both of these organizations treat highly classified material. Additional physical security measures are included for these organizations to ensure that only those employees working in NSD and IG CSIS have access to their respective working areas. Any visitors require an escort at all times.

The Department has also implemented codetronic locks to secure doors leading to sensitive areas. For example, these locks are employed on doors leading to the LAN server rooms as well as to records management areas. The audit team has found that these doors are always locked if unattended.

Observation 5.9.1

[

16(2)(c)

]

[

16(2)(c)

]

Recommendation 5.9.1

[

16(2)(c)

]

Observation 5.9.2

[

16(2)(c)

]

5.9.3 STUIII Phones

The Department currently has 70 STUIII phones of which 50 are active. There are a number of administrative procedures surrounding these items, as they are sensitive assets. For example, users must update their keys every four months. The ADSO keeps track of all keys for the phones in use.

[

16(2)(c)

]

The audit team suggests that the need for each phone should be reviewed when the next inventory is taken. If some of the phones are not required, they could be eliminated from the inventory, thus removing some of the workload surrounding them.

5.9.4 Combination Numbers for Safes, Padlocks, and Doors

The Department extensively uses safes and filing cabinets with padlocks for protecting sensitive information. Safes are used for storing classified information at the Top Secret level and above while padlocked cabinets are used for other sensitive information. As mentioned above, codetronic locks are also used in some areas of the Department.

[

16(2)(c)

]

Observation 5.9.3

With approximately 450 combinations for all the locks in the Department, their management has become a rigorous and tedious exercise. As mentioned previously, the Security Clerk's workload is quite high and this exercise is one that takes a lot of the clerk's time. [16(2)(c)

]

Recommendation 5.9.2

In order to reduce the workload surrounding the management of the combination locks, the Department should consider the following:

- **Changing those locks for organizations that treat less sensitive information (below Top Secret) once per year instead of twice (maintain the twice per year schedule for NSD and IG CSIS);**
- **Create a unique envelope per Directorate only rather than for each lock. This would help in reducing the administrative workload for changing the combinations.**

5.10 Records Management

The security practices surrounding the handling of hard copy information is well implemented within the Department and complies with the GSP. Files are properly classified, stored, transported, archived and destroyed in accordance to the directives. Employees are well aware of the sensitive nature of the information that they have access to and generally apply the directives correctly.

Good management and operational practices were observed in the central records office and the sub-records offices. Procedures relating to the lending of documents and files allow tracking of file movement and provide assurance that the borrower's security clearance level is appropriate for the file requested. The Records Information Management System (RIMS) is updated with the personnel's security clearance level and it is accessed for verification before lending a file out.

The Department has a classification guideline for documents and it is used appropriately within the Department. In the operational units, employees are well aware of the nature of the information that they manipulate and correctly classify paper documents.

Observation 5.10.1

[

16(2)(c)

]

Observation 5.10.2

[

16(2)(c)

]

Generally, information that is stored on a Directorate's shared LAN drive (i.e. G:) is available to any employee within that Directorate. Although most people are cleared at the same level, some temporary help may not. These documents are also available to those employees working from home at times.

Recommendation 5.10.2

The GSP is very clear on the proper way to create, store, and print classified electronic information. The Department should ensure that all users comply with the policy. We recommend the following:

- **That the awareness of employees be increased on this issue through the briefing sessions and through other means as best seen fit.**
- **That the Department undertakes "sweeps" of the non-classified LAN drives in order to identify documents that are stored inappropriately. Any breaches identified should be reported to the user and also to the Director General of the unit.**

Observation 5.10.3

As is the case in most federal government departments, the Department uses electronic mail extensively to facilitate communication internally and externally. Email is not to be used for the transmission of sensitive information and certainly not for any classified information. [

16(2)(c)

]

Recommendation 5.10.3

It is very difficult (if not impossible) to monitor the information transmitted via email. However, the Department should increase the employees' awareness about this issue in order to minimize the Department's risk related to the practice.

5.11 Access to Information and Privacy (ATIP)

As with any other federal government department, the Department is subject to Access to Information requests. The ATIP unit has been given the responsibility for managing the entire process from the time that a request is received to the actual delivery of information (as is the case). The audit team has found that the process used to satisfy such requests is good.

Generally, a request is received in the unit. Once validated, it is sent to all the directorates, which may have information related to the request. The information is collected by the responsible manager and is sent to the ATIP unit for vetting. The manager may be involved in the vetting process depending upon the information. Once completed, the information is sent to the requestor and a copy is kept in filing cabinets in a room on the first floor. This room is accessible by the general public who wish to view previous ATIP requests and their responses.

Observation 5.11.1

Individuals from the public have complete access to the previous ATIP requests and responses from the Department as the documents are stored freely in a room on the first floor. This is fine, as these documents are public knowledge. However, a person can take any document away with him without advising anybody. As these are the only copies of the requests and responses kept, the Department can loose track of this information and may have to recreate it in the future.

Recommendation 5.11.1

Signs should be posted in the ATIP room informing visitors that documents are not to be removed from the room but that copies can be requested for removal, if desired.

5.12 Information Technology

During the initial stages of the audit, it was decided that IT Security should not be looked at in detail so that the audit could focus on other aspects of security within the Department. Therefore, the audit team only did a cursory review of the IT portion of security.

5.12.1 Desktop Security

The Department is currently running Windows 95 (Win95) as their standard desktop Operating System (OS). Although the Systems Division would like to migrate to Windows 2000, the Department has not made any financial commitment to support this. A TBS submission was made earlier that includes the new OS but approval has not yet been received.

Observation 5.12.1

[

16(2)(c)

]

Observation 5.12.2

The Department's security manual states that passwords should be at least six characters long, be changed regularly, be composed of both letters and numbers, and should not be words easily recognizable. Also, the same password should not be used for two purposes and should not be written down and kept close to the workstation or in the person's wallet, purse, etc. [

16(2)(c)

]

The effective use of passwords is a challenge for most organizations. Independent studies have found that the more complicated passwords get, the more users need to write them down and keep them close by thus increasing the risk of unauthorized access. The Systems Division wishes to eliminate passwords altogether for most desktop users by implementing a more secure environment consisting of Win2000, PKI with strong authentication using smart card and biometrics (such as thumb print) technologies. This combination would resolve the problem of the screen saver and passwords for the Department. It would also provide a number of other benefits to secure data and communication at the Protected B level. Unfortunately, a PKI platform has not yet been approved by the Communications Security Establishment (CSE) or the RCMP that would allow for the storage and transmission of classified information. A project, which addresses the transmission part, is currently underway at CSE called "Classified Messaging" but the results of this are not expected for another 2 years.

Recommendation 5.12.1

We recommend that the Department pursue the Systems Division's plans of implementing a more secure environment through the use of Win2000, PKI, smart card and biometrics technologies. Although this will not resolve the problems related to classified information, it will resolve the problems associated to desktop security and passwords and position the Department for the eventual solution coming from CSE for classified messaging.

APPENDIX A

LIST OF INTERVIEWEES

The following people were interviewed as part of the audit.

Ms. Eva Plunkett	DG, Corporate Services (DSO)
Ms. Debbie Cuerrier	Director, Administration (ADSO)
Mr. Gregg Murphy	ITSO
Ms. Darryl Donald	Security Clerk
Mr. Dean Clisch	Administration Officer, APD
Ms. Ruth Hawkins	Senior Review Officer, IG CSIS
Mr. Serge Bériault	Advisor, Integrated Justice
Ms. Joanne Laframboise	Human Resources Assistant
Ms. Erin Robinson	Contract/Procurement Officer
Ms. Linda Chapman	Chief, Staffing & Staff Relations
Mr. J.P. Bissonnette	Chief, Human Resources Development
Mr. Daniel Lemieux	Manager, Records Systems & Operations
Mr. Dave Rooney	Records Management Clerk – Sub Records Office
Mr. George Holmes	Records Management Clerk – Sub Records Office
Mr. Duncan Roberts	Head, ATIP Unit
Mr. Gerry Léger	Director, Systems
Mr. Michel D'Avignon	DG, National Security
Mr. Jamie Deacon	Director, Anti-Organized Crime, PLED
Mr.Jim Bonta	Chief, Corrections Research
Ms. Lynda Clairmont	Director, Operations & Policy, APD
Mr. Ian Blackie	Senior Policy Analyst, NSD
Mr. John Clark	Director, Policing, PLED
Ms. Lucie Baulne	Briefing Officer, Executive Services