NSERC CRSNG

Investing in people, discovery and innovation
Investir dans les gens, la découverte et l'innovation

Follow Up – Audit of Security (August 2001)
As of November 2002

Prepared by Nathalie J. Meilleur – Senior Internal Auditor
Version 1.2

Table of Contents

Version Control

Version Control	Date	Completed by	Changes made
1.0	Nov 7, 2002	Nathalie J. Meilleur	Creation of document
1.1	Nov 19, 2002	Nathalie J. Meilleur	Comments received from René, Martha and Cliff
1.2	Nov 20, 2002	Nathalie J. Meilleur	Approved by Management Committee

Introduction

Purpose

In the summer 2001, a Security audit was conducted by Progestic international inc. The audit was a joint audit for NSERC and SSHRC. The purpose of the 2001 audit was to assess the effectiveness and efficiency of security measures and their compliance with Government Security Policy and Operational standards.

The purpose of this follow up is to assess progress made on recommendations raised by the audit and evaluate management actions.

Scope

The follow up is not an audit, and will not reassess effectiveness and efficiency of security measures at this point in time. The follow up is intended to provide to NSERC audit committee an overview of security activities undertaken since the audit and to identify continued exposure to security risks within NSERC. The follow up was specific to NSERC only.

Approach

The assessment of progress was primarily based on discussions with key individual (Appendix A) at NSERC that support the security function and a review of relevant documents. The progress has been recorded in the Management Responses Follow Up Verification Sheet (Appendix B). For each recommendation and management response raised in the 2001 audit a brief description of the progress is included as well as the status for each recommendation. The status is either C = CLOSED where recommendation has been fully implemented or O = OPEN where recommendation is pending.

Security Context

In August 2001, the security context was quite different. Since then, several events have reshaped the way we look at Security. The repercussions of September 11, 2001 and the various terrorism activities across the world have redefined Security. The Government of Canada has responded with several initiatives including a new Government Security Policy (GSP) dated February 2002.

This policy identifies new security baseline requirements that must be put in place at NSERC. In addition to the recommendations made in the audit report, the new requirements must also be incorporated as well. A list of the security requirements under the GSP is included (Appendix C).

While the follow up assesses progress against recommendations made in the 2001 audit report, the Senior Internal Auditor recognizes that the security context has changed and that new priorities have emerged which have shifted the focus.

Major activities undertaken since the 2001 audit report

The focus of NSERC in the last year has been to review the entire security function structure and clearly define the security roles and responsibilities across NSERC and CASD. A security organizational design review is currently underway by CASD. The purpose of the review is to:

- Determine the best organizational structure for the security functions;
- Clarify the security roles and responsibilities; and
- Identify compliance gaps with the new Government Security Policy.

At the time of the follow up the results of the organizational design review were not known.

While focused on the organizational design review, some progress on Security has been made. Appendix B provides a short description of the progress made against each recommendation. In some cases progress has been delayed and is awaiting the results of the organizational design review before being fully implemented.

Major activities include:

- An organizational design review which is currently underway;
- A gap analysis of the new Government Security Policy has been conducted;
- Roles and responsibilities have been clarified in the draft NSERC security policy and staff job descriptions. Further clarification expected from the review study;
- Additional security procedures have been drafted; and
- Specific groups within NSERC have taken security training and other groups have been identified for targeted training.

Continued exposure to security risks

Several recommendations made in the audit reports have yet to be implemented and in some cases the delay is justified based on the recent changes. Meanwhile, NSERC continues to be exposed to security risks that should be closely monitored. Those areas of greater concern to NSERC include:

- The Council continues to transfer application material by e-mail, either by attachments or by electronic files, without encryption.
- Staff awareness of security measures continues to be low. No effective security program is in place for NSERC.
- Security roles and responsibilities continue to be unclear at various levels at NSERC (i.e.: managers responsibility; IT security, etc…).

- There is no business continuity planning for NSERC.
- Security requirements are not met in contract management.

Conclusion

While the last year has demonstrated slow but steady progress in Security, significant effort is still required to meet the basic requirements. However, it is apparent that necessary steps are being taken to build a strong security foundation (organizational structure) for NSERC. It is not known if the organizational design review will have a significant impact; until the results are known it is difficult to estimate changes required to the security function and roles and responsibilities. Progress should be closely monitored by management in order to ensure that the security risks are known and managed adequately.

Next steps

A Security Audit is expected to be conducted every 5 years. The next audit should be scheduled for 2006. While we anticipate significant change in Security in the next few years, I would recommend another follow up in 2004. This will provide sufficient time to fully implement the results of the organizational design review, the requirements of the new Government Security Policy and the audit recommendations.

Appendix A

Individuals consulted for the follow up

Name	Affiliation
René Quirouette	Director, Administration Division and DSO
Martha Heyerdahl	Coordinator, Security and Projects
Cliff Moore	Technical Services Manager (IT Security Coordinator)
Daniel Blain	Support Centre Manager

Appendix B
Management Responses Follow Up Verification Sheet

	Recommendation	Management Response	Progress	O / C
Management Control Framework				
Security Organization				
1	The security organisation and reporting relationships should be formalised and documented and security responsibilities and tasks should be documented as part of the overall Security Policy. Security responsibilities should be prepared for all security staff members and all others involved in the security function, including the security responsibilities of end-users. Priority immediate (within the next three months	Agreed. A draft security policy has been written proposing roles and responsibilities. We recommend an organisational review of security function to propose a formal delivery structure. In the interim, staff responsibilities are being identified as we progress on the development of procedures for the proposed Council intranet. Planning is underway to include an awareness document for new hires to be delivered during the security clearance process	An organization design review for the security function is currently underway. The study will address organizational structure, roles and responsibilities, and the requirements under the new Government Security Policy (Feb 2002). The study is expected to be completed by end of November. Meanwhile, the roles and responsibilities have been further defined through different initiatives: • the draft of the Security policy (Jul 2002) started to define roles and responsibilities; • the job description exercise has provided some clarification (including in ISD); The Security policy will be amended and reflect the findings of the organisation design review. Elements of the document for new hires have been identified but must be further developed for the Health, Safety and Security Administrator to deliver during one on one security briefings with staff.	O
Security Requirements Checklist (SRCL)				
2	The SRCL should be completed for all contracts. Priority immediate (within the next three months)	A review of contracting requirements fulfilling the Council's operational and project requirements will be undertaken within the context of a threat and risk assessment. Contract requirements with security requirements will be identified and any policy and procedural outcomes will be addressed with	The SRCL checklist is a federal form. The checklist has yet to be added to the NSERC contracting process.	O

	Recommendation	Management Response	Progress	O / C
		management and promulgated. Given the other priorities, this requirement will not be addressed until the second quarter of the new fiscal year		
Security Policy and Formalized Security Procedures				
3	The Security Function should ensure that an integrated and comprehensive security policy and associated procedures be completed. Priority immediate (within the next three months)	Agreed. A draft policy document has been completed and the roles and responsibilities are being reviewed prior to proceeding with the remainder of the policy	A second version of the draft policy has been completed. This new version includes elements of the requirements under the new Government Security Policy (Feb 2002) . This version also includes some procedures. The policy will be kept in draft until the results of the organization design review are known. The results will be incorporated in the policy.	O
4	In order to facilitate its communication across the Councils, Security should develop a security topic within the Intranet Site where policies, procedures, guidelines and standards are detailed for all staff to read. Priority immediate (within the next three months	Agreed. Procedures have already been developed and communicated. The emergence of the Council's intranet will provide with an important opportunity to enhance our communications with staff	The first release of the Intranet Pilot was not structured in a way to easily post procedures for staff. Some procedures have been developed, but those remain on paper copies and have yet to be distributed to staff. It is expected that the next release of the Intranet Pilot will include some security procedures. It is scheduled for release in November.	O
Reporting of Incidents				
5	The security policy and procedures should include security incident reporting. The Security Function should clarify what is a security incident (IT and non-IT related). The definition should be non-ambiguous and precise. Priority immediate (within the next three months)	Agreed, this will form part of the security policy and procedures currently under development	Draft Policy on Administrative Investigations has been completed and awaits the results of the aforementioned Security Review prior to its promulgation. A draft reporting procedure for IT incidents has been completed as well and will be incorporated into an IT Security Policy – an adjunct to the Security Policy. "Incidents" term has not been defined, and no standard format has been developed. Judgement is used in the development of the incident reports.	O

	Recommendation	Management Response	Progress	O / C
Disaster Recovery / Business Resumption Plans				
6	The Program Branches, together with the Security should develop the Business Resumption and Disaster Recovery Plans as soon as possible (without a two to three year delay). Such plans should include several levels of disaster scenarios and appropriate responses and technical, physical and resource requirements as well as readiness test plans. Priority soon within the next six months)	Agreed. An IT Disaster Recovery Plan (DRP) exists. Narrower in scope than a Business Resumption Plan, the IT DRP focuses on roles, responsibilities, and activities required to reconstitute our IT infrastructure to enable the Council to carry on its business. The IT DRP will form part of the Business Resumption Plan, which has yet to be done. While we agree it is a priority and should be addressed sooner than the original timeline, the corporate nature of this project will likely schedule the plan for the 2nd quarter of the next fiscal year	Due to the introduction of the new Government Security Policy and Sept 11 events, no progress has been made to the development of a Business Resumption Plan. It is considered to be the next major priority after the organization design review. This initiative is expected to start within the next three months. The IT DRP is out of date and should be updated with appropriate contacts and include e-business activities.	O
Records Management				
7	A statement of sensitivity and relevant injury tests should be carried out to determine the designation/classification of grantees' research results and papers and a Threat and Risk Assessment should be completed to determine the appropriate protection to be given both in transmission, handling and storage. Priority soon (within the next six months)	Agreed. A threat and risk assessment of our information holdings, which will include a statement of sensitivity and relevant injury tests is scheduled to be started before the end of the calendar year. The end product will provide guidance in the appropriate safeguards to be used in collecting, storing, transmitting and disposing of our information	Closely related to the Records Management initiative underway. As a result, no progress has been made until the action plan for the Record Management initiative has been finalized. A strategic plan was presented to Management Committee on November 4, 2002.	O
Security Awareness				
8	The Security function should develop a security awareness program. This program should be in a progressive manner so that new staff receive a security briefing shortly after initiating work and that other staff receive refresher sessions on a regular basis. Priority soon (within the next six months)	Agree. Planning is underway to include an awareness document for new hires to be delivered during the security interview and clearance process. Security does not have the resources to offer refresher sessions on a regular basis, but we will be using the Council's intranet and security bulletins to remind staff of their security responsibilities	Some elements are in place, but no awareness program has yet to be developed for the staff. It is on the workplan, but at this time, it is not clear when this activity will start. Some managers (approx. 5) have gone on security awareness courses.	O
Physical Security				
IT Inventory				
9	A pool of laptop computers should be established for temporary loan to employees for	A pool of laptops, which can be borrowed from the ISD Helpdesk, has existed for several years		C

	Recommendation	Management Response	Progress	O / C
	business trips. Priority immediate (within the next three months)			
10	These computers should be security "wiped" after each loan and control established over what level of data is installed. Priority immediate (within the next three months)	Agreed. Information Services Division staff will be examining available products and implementing procedures	For the last year and a half, a procedure is in place to have all laptop hard disks erased with a new image. However, these are not security wiped, and with appropriate technology, erased information could be restored from laptops.	C
11	Furthermore only certain individuals should be given the responsibility of authorising the signing out of pool laptops to employees, therefore establishing a minimum level of inventory control. Priority immediate (within the next three months).	All loans are recorded and only helpdesk staff can authorise and record an equipment loan. However, a large number of laptops are on permanent loan or in departmental pools managed by groups outside of ISD. These are not necessarily closely controlled. This arrangement will be reviewed in the next six months.	Still some laptops managed outside of ISD, but those are reducing in number. ISD no longer supports laptops managed outside of ISD. It is expected that by next year, all laptops will be managed by ISD.	O
Emergency Evacuation Procedures				
12	The Security should develop foolproof procedures to ensure that two lists of persons requiring assistance be maintained: permanent assistance, and temporary assistance. Priority immediate (within the next three months)	Lists of permanently and temporarily mobility impaired persons requiring assistance is complete to the extent that we have been advised. Reporting one self as mobility impaired is voluntary. The Emergency Response Team meets with staff whose mobility impairment precludes them from using the stairs in order to establish a personal evacuation plan. Within the next six months, we will target awareness initiatives to increase the level of reporting	Remind mechanism are in place to have people report one self as mobility impaired. Three consultations to develop individual evacuation plans for the unique needs of specific mobility impaired staff have taken place in the last year.	C
13	In addition, the Emergency Evacuation Plan should be posted in prominent locations on each SSHRC/NSERC floor. Priority immediate (within the next three months)	Agreed. Significant facility upgrades are underway at the moment, that may cause minor delays in posting plans on all Council floors, but the need has been identified to be addressed within the next three months	A draft of the floor plan has been developed, but not posted on each floor. Need to resolve whether the responsibilities lies with the building owner or the Council for posting.	O
IT Security				
Logging and Auditing				
14	Logging and auditing should be turned on at all	Until recently, logs were only reviewed as	Logs are maintained for most critical areas:	O

	Recommendation	Management Response	Progress	O / C
	times and in all cases, and the logs reviewed by the IT Security on a frequent and regular basis. There is a need for tools to enable critical log entries to be highlighted or parsed and such tools should be purchased as soon as possible. Priority immediate (within the next three months).	needed, but since a new position has been staffed with security as a primary focus, logs and statistics are being reviewed daily and suspicious events are followed up. Vulnerability analysis software has been purchased and is starting to be regularly used. Intrusion detection software has been purchased, and will be implemented this fiscal year	antivirus, etc… Still investigating tools for the firewall. A full time IT security analysis reviews the logs and follows up on incidents. The Intrusion system is in place but has yet to be fully configure for optimal use. Limited logging being monitored on individual corporate systems (i.e.: NAMIS, FPAM).	
15	Log files should be retained for a fixed period (e.g. 30 days) if there are no security breaches and indefinitely if there has been a breach or indication of a breach. Priority immediate (within the next three months).	We agree log files should be retained for 30 days if there are no security breaches, however, as with all government records, even log files where a security breach has been identified must have a definite retention period. We will consult with the Recorded Information Division for recommended retention periods	Logs are kept at least 30 days. Discussion with Recorded Information Division has yet to take place.	O
16	All dial-in access should be via the firewall thus forcing verification on dial-in access and allowing that access to be restricted. Priority immediate (within the next three months).	A security-consulting firm was contracted to recommend a secure solution to replace the existing remote access method. A three-tiered solution was recommended (OWA e-mail + terminal services applications + full VPN access), the first tier of which has already been implemented (OWA e-mail), and a project has started to begin weaning staff from the existing RAS access solution	Significant foundation work has been done through the teleworking group (potential users of dial up access). Security has been tightened up on dial up access. While framework is in place, a technical solution has yet to be identified and implemented. The teleworking policy still needs approval from a few committees in the Council.	O
17	SSHRC and NSERC security policy and procedures should contain a clause forbidding any unauthorised use of a modem except for dial-in access from outside of the Councils premises. Priority immediate (within the next three months).	All laptops use internal modems to connect to the Council's network. A risk assessment on this usage will be done next fiscal year. The Council Security Policy will include a clause forbidding unauthorised use of dial-in access	From a user perspective, very little progress has been made. At this time, they have looked at the Corporate Systems.	O
IT Monitoring				
18	Users should be warned by an appropriate logon banner, that surveillance is in effect. Priority soon (within the next six months).	This has been done. All new users work stations have been configured to display a logon banner every day for a week reminding them of their security responsibilities and the consequences of	Security banners appears at logon for new employees for the first few months.	C

	Recommendation	Management Response	Progress	O / C
		inappropriate use		
Threat and Risk Assessments				
19	Threat and Risk Assessments including Statements of Sensitivity and development of security requirements and specifications should be carried out early in the systems development life cycle, beginning with the system initiatives currently under development. Priority immediate (within the next three months)	Agreed. Much of the success of implementing this requirement will depend upon the scope and authority of the IT security function and how it is implemented in the Council We have identified the requirement to conduct a threat and risk assessment for the NSERC's E-business initiative, this will start in November 2001. A similar initiative at SSHRC will be addressed when the IT security function is resourced	A TRA has been done for e-business initiative. The Government Security Policy describes the TRA requirements and format. There is currently no guidance for smaller initiatives. ISD is trying to tailor the approach to different situations.	O
External Telecommunications				
20	All designated telecommunications (by telephone or radio) by employees from external locations should be encrypted utilising PKI which has already been partially deployed. Priority immediate (within the next three months)	In fact, there is only one handheld messaging device that has been deployed to date. PKI is not an encryption technology – it is an authentication system using software, practices and individual certification. Generally, it is more applicable to electronic communication over the Internet than to telephone or radio. We will, however, be investigating government-approved software for securing telecommunications within the next six months	No safeguards in place at this time. Mostly based on procedures rather than technology. No specific procedures have been issued on the use of these devices (i.e. blackberry) and the security impact.	O
Disposal of Computer Equipment				
21	We recommend that the Security issue a procedure to ensure that data contained on PCs, tapes, hard disks, removable hard disks to be disposed of, must be properly sanitised using a recognised and acceptable sanitation method similar to the one presented in Appendix B. Priority immediate (within the next three months)	Although special hardware/software methods are not yet used to sanitise computers, hard disks are formatted before being declared surplus. ISD sends all surplus diskettes, tapes and commercial software for secure destruction. Within the next six months, we will be investigating approved software for wiping or sanitising hard disks	In the case of servers, drives are taken out and sent for secure destruction. In the case of computers, drives are erased. However, with appropriate technology, erased information could be retrieved from the hard disk. No progress made on investigating approved software for wiping or sanitising hard disks.	O
Secure Communications				
22	Security should conduct a comprehensive Threat and Risk Assessment covering the transmission	This Threat and Risk Assessment has been done and has recommended the implementation of a	No progress made to date.	O

	Recommendation	Management Response	Progress	O / C
	of sensitive information over unsecured lines to an unsecured recipient. Priority immediate (within the next three months	Public Key Infrastructure system such as the one now in use in the Federal Government. However, this poses a number of challenges for the Council, not the least of which, is the implementation of this technology within the Council and in our client community. We will be addressing these and other significant issues as we progress with the Council's e-business initiatives. In the interim, we have migrated some of the typical e-mail based communication to a more secure environment on our web site. However, we are still faced with securing electronic communications between Council staff and our community (universities, companies, individuals, etc.). We will continue to consult with security experts within government and industry to seek viable solutions		
23	Until the conclusions of the TRA are known, we recommend that the private courier and registered mail techniques be used to transmit applications for grants and examination by external evaluators. Priority soon (within the next six months).	Standards for the protection of information will be a result of the information security threat and risk assessment targeted to start within the next two months. Interim guidance is provided on a case by case basis	There is currently a pilot project under the e-business initiative. No formal TRA has been done. A statement of sensitivity has been done by the e-business project group.	
24	The Security should review the faxing of sensitive information and develop appropriate security procedures that comply with the GSP rules and guidelines. Furthermore, security awareness program should address this issue. Priority soon (within the next six months).	Standards for the protection of information will be a result of the information security threat and risk assessment targeted to start within the next two months. Interim guidance is provided on a case by case basis	No progress made to date.	O
Passwords				
25	Enhanced password rules should be put in place and enforced	Users are currently required to change their password every 90 days		C
Pornographic / Hate Material via Internet				
26	All internet activity file downloads (by file name) and hard disks (again for file name) should be monitored both on-line and by review	This will require a change to current council policy. Council has explicitly decided to trust the professionalism of staff and not to monitor	Council is still relying on the trust of professionals and do not monitor daily activities. The matter has not been raised with	C

	Recommendation	Management Response	Progress	O / C
	of the firewall logs. Monitoring, in this context, does not mean that user files or messages are opened but only that IP addresses accessed by the user are checked and possibly, the sites that they accessed are reviewed, only if the logs indicate that there has been access to inappropriate sites. The above subject matters should be included in the policy and procedures currently under development. Priority immediate (within three months).	daily activities. Monitoring occurs only as a result of suspected inappropriate or criminal activity that may be reported by staff. However, issues of liability, especially in civil or criminal cases, may require a more active monitoring program. The matter will be put before management for further consideration before the end of this fiscal year	management to review this decision. Scanning is being done on incoming e-mails based on key words and virus scans.	
User Accounts - Inactive				
27	When employees do not or will not access their user-Ids without extenuating circumstances, for a period, say 60 days, the IT Security should revoke or suspend their accounts. Priority immediate (within three months).	The ISD Helpdesk and Technical Services regularly review network accounts and disable those that have been inactive for extended time periods. The IMEP (Intake Modification and Exit Process) exit procedure ensures that all reported accounts are disabled when staff leave	In addition to the process in place, periodic scanning is being done by ISD.	C
Personnel				
Hiring and Termination of Staff				
28	Security should develop procedures that will provide guidance to managers in relation to the disposal of any e-mails, files or other information left on Council computers or other storage means upon employees terminating employment. Priority immediate (within three months).	Procedures have been established through the implementation of the Council's Intake, Movement and Exit Process (IMEP). It provides guidance to the manager with regard to the handling and disposal of e-mails and personal storage. ISD deals with personal storage based on directions from the departing employee's manager		C
Contractors				
29	All contractors should be subject to a SRCL and that their level of security clearance should be ascertained and deemed appropriate prior to contract start. Priority immediate (within the next three months).	Agreed. See response to 3.1.2.	Refer to 2.	O
Protection of Staff				
30	Employees, when meeting with individuals who	This advice has been the subject a regular e-	An Employee Security Guide has not been	O

	Recommendation	Management Response	Progress	O / C
	have given an indication that they may be fractious or threatening, should be accompanied by another employee or by a responsible individual who is not an employee. Priority immediate (within three months).	mails to all staff, and will be included in the Employee Security Guide which is currently under development. The Guide will take the form of a document as well as be posted in the Council's Intranet	developed. The Security Coordinator, Learning Advisor and program staff (Investigations and Monitoring, Finance Division) have identified an appropriate course on employee safety as it relates to client interaction Staff and the Learning Advisor are finalizing details on registration. Similar discussions will need to take place within the Council (i.e.: Research Grants Staff) with different groups.	
31	As a matter of urgency, the two Councils develop a joint procedure for dealing with individuals who are fractious or threatening. Such procedures should detail the steps to be taken and also the circumstances under which the police should be called. Priority immediate (within three months).	This advice has been dispensed on a case by case basis, however, it will also be included in the Employee Security Guide which is currently under development. The Guide will take the form of a document as well as be posted in the Council's intranet	No progress made to date.	O
32	Employees, who regularly meet with grant applicants, attend courses such as "Conflict Management", "Violence in the Workplace" and "Dealing with Difficult Individuals" as part of their professional development. Priority immediate (within three months).	Agreed. Security will work in concert with our HR Training advisor to integrate this training as part of Council staff's professional development	Communication with the Learning Advisor has started. Need to identify the different groups within the Council and identify appropriate courses for recommendation.	O
33	NSERC and SSHRC develop procedures for the mailroom covering the handling of questionable parcels and letters. Such procedures should include the name of the person to call, when to call police, fire, medical and other authorities. Priority immediate (within three months).	A guide to responding to questionable material received in the mailroom has already by distributed to our Mail Operations staff. This will be followed up with formalised training	A reminder was sent to the general population. Mailroom activity is centralized and procedures are posted in the mailroom.	C

Appendix C

Requirements under the new Government Security Policy

	Requirements
1	Security program
2	Sharing of information and other assets
3	Security outside of Canada
4	Contracting
5	Security training, awareness and briefings
6	Identification of assets
7	Security risk management
8	Access limitations
9	Security screening
10	Protection of employees
11	Physical security
12	Information technology security
13	Security in emergency and increase threat situations
14	Business continuity planning
15	Investigation of security incidents
16	Sanctions