

Additional Information for GNWT Response to CR 1-17(3): Review of NWT Information and Privacy Commissioner's 2010-11 Annual Report

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
<p>Report on the Review of the Information and Privacy Commissioner's 2006/2007 and 2007/2008 Annual Reports Tabled October 22, 2009 GNWT Response Tabled February 17, 2010 <i>** For clarity in reporting, the GNWT responded to Standing Committee's first recommendation in two parts (1a and 1b)</i></p>			
<p><u>Recommendation 1A</u> The Standing Committee on Government Operations recommends that the GNWT establish policies on routine and active disclosure of public records, following best practises in other parts of Canada. (Committee Report 1-16(4); page 2)</p>	<p><i>The GNWT recognizes the public is better served and better informed when the principals of routine disclosure and active dissemination are applied appropriately. Public bodies also benefit by avoiding the high cost of processing individual access-to-information requests.</i></p> <p><i>The current ATIPP Policy and Guidelines Manual details procedures that access and privacy coordinators may follow to create routine disclosure and active dissemination practices specific to their public bodies. The establishment of these practices is an important part of a public body's commitment to an open exchange of information with the public that it serves.</i></p> <p><i>The GNWT will continue to encourage public bodies to be proactive in establishing practices that foster routine disclosure and active dissemination. The Department of Justice will commit to reviewing the ATIPP Policy and Guidelines Manual sections that are specific to information disclosure and dissemination to ensure the manual provides sufficient direction to public bodies in this regard. The manual is expected to be updated by spring 2010, with distribution to GNWT access and privacy coordinators through the Access and Privacy Administration Committee.</i></p>	<p>The Department of Justice reviewed and updated the ATIPP Policy and Guidelines Manual Appendix 4 - Routine Disclosure and Active Dissemination.</p> <p>The updated section emphasizes that public bodies should be proactive in establishing practices or policies that foster routine disclosure and active dissemination.</p> <p>The revised section was distributed to Access and Privacy Coordinators at the June 10, 2010 Access and Privacy Administration Committee meeting, with a follow up discussion at the October 17, 2010 meeting.</p> <p>Public bodies were also informed that additional assistance on this matter is available through the GNWT Access and Privacy Office.</p>	<ul style="list-style-type: none"> • Sections of the ATIPP Policy and Guidelines Manual continue to be updated and distributed as required. • A new edition of the manual will be completed following the comprehensive review of the ATIPP Act. <p>The GNWT considers its response to this recommendation completed.</p>

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
<p><u>Recommendation 1B</u></p> <p>The Standing Committee on Government Operations recommends even though discretionary exemptions exist that allow public bodies to withhold information, in situations where information is withheld, a full explanation of the rationale for the decision should be provided as a matter of course.</p> <p>(Committee Report 1-16(4); page 2)</p>	<p><i>The ATIPP Act (Section 9-1ci) requires public bodies to provide applicants the reason for refusing them information, citing specific sections of the Act which support the refusal. This is required for both discretionary exemptions, where the head of the public body may exercise discretion regarding disclosures of information, and mandatory exemptions, where the head must refuse to disclose information.</i></p> <p><i>The GNWT recognizes the importance of providing rationale to applicants. The Department of Justice will commit to reviewing the appropriate sections of the ATIPP Policy and Guidelines Manual to ensure these requirements are clear for public bodies to follow. As noted previously, the revised ATIPP Policy and Guidelines Manual is expected to be updated and distributed by spring 2010.</i></p>	<p>The GNWT Access and Privacy Office reviewed the appropriate sections of the ATIPP Policy and Guidelines Manual to ensure the requirement to provide the rationale for decisions denying access is plainly stated.</p> <p>The manual clearly indicates applicants who have been denied all or partial information requested, must be provided the reasons for the refusal and the section of the ATIPP Act on which the refusal is based. The section further indicates this is required for both mandatory and discretionary exceptions. To ensure clarity on this matter, the model letters which are used by Coordinators as a template for responding to applicants, were revised to emphasize this requirement.</p> <p>This item was discussed at the June 2010 Access and Privacy Administration Committee meeting and the revised model letters were distributed.</p> <p>Public bodies were also informed that additional assistance on this matter remains available through the GNWT Access and Privacy Office.</p>	<ul style="list-style-type: none"> Sections of the ATIPP Policy and Guidelines Manual continue to be updated and distributed as required. A new edition of the manual will be completed following the comprehensive review of the ATIPP Act. <p>The GNWT considers its response to this recommendation completed.</p>
<p><u>Recommendation 2</u></p> <p>The Standing Committee on Government Operations recommends that the GNWT enhance its policies and guidelines on the use of portable electronic devices and the access and privacy issues that arise through the use of such devices.</p> <p>(Committee Report 1-16(4); page 2)</p>	<p><i>The GNWT recognizes mobile handheld devices are tools that assist employees in the performance of their duties; however, users must comply with government legislation, policies and guidelines related to use of these devices.</i></p> <p><i>To clarify responsibilities of employees using devices such as cell phones, smart phones or personal digital assistants, the Informatics Policy Council approved the Mobile Handheld Devices Policy 6003.08.10. Employees using these devices are advised information transmitted or received on these devices are considered a government record and therefore subject to the access and privacy provisions of the ATIPP Act. The policy</i></p>	<p><i>The Mobile Handheld Devices Policy 6003.08.10 and the Electronic Information Security Policy 6003.00.26 continue to be the applicable policies and guidelines addressing the use of electronic devices in the GNWT.</i></p> <p><i>The Electronic Information Security Policy 6003.00.26 was initially under review with the GNWT Security Officers Committee, however due to a staffing vacancy in the Chief Information Security Manager position, the committee is currently inactive. The Office of the Chief</i></p>	<ul style="list-style-type: none"> The <i>Electronic Information Security Policy 6003.00.26</i> and its supporting guidelines will be reviewed as resources become available. OCIO - Recruitment of a GNWT Information Security Manager and two supporting Security Analysts will be

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
	<p><i>informs employees of their responsibility for the security of the personal information held on these devices. The policy also addresses asset and records management, security considerations and terms of acceptable use.</i></p> <p><i>Access and privacy considerations for portable electronic devices such as laptops and flash drives are currently covered under the Electronic Information Security Policy 6003.00.26. The policy provides direction on implementing information security standards, guidelines and procedures. The policy and supporting guidelines are currently under review with the GNWT Security Officers Committee.</i></p>	<p>Information Officer, (OCIO) Finance has indicated the policy and supporting guidelines will be reviewed, as resources become available.</p> <p>However, the OCIO is currently working on a proposed Mobility Strategy that will address the use of portable electronic devices and the access and privacy issues associated with these devices.</p>	<p>undertaken in 2012-13.</p> <ul style="list-style-type: none"> OCIO - The proposed Mobility Strategy is anticipated to be completed in Spring 2013-2014.
<p><u>Recommendation 3</u></p> <p><i>The Standing Committee on Government Operations recommends that the GNWT undertake a comprehensive analysis of the review of the Personal Information Protection and Electronic Documents Act [PIPEDA] to determine the need for GNWT legislation to protect the personal information of the people of the NWT held by the private sector.</i></p> <p><i>(Committee Report 1-16(4); page 3)</i></p>	<p>The Federal Standing Committee on Access to Information, Privacy and Ethics initiated a review of the federal legislation (PIPEDA) in November 2006 and completed public hearings in February 2007. Their report, the <i>Statutory Review of the Personal Information Protection and Electronic Documents Act, Fourth Report</i>, was tabled in May 2007 in the House of Commons. The federal government tabled their response to this report, titled <i>Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics</i>, on October 2007. The response addressed the 25 recommendations put forward by the federal standing committee.</p> <p>GNWT Justice committed to review the federal government's response and report back to the 15th Legislative Assembly Standing Committee on Accountability and Oversight in fall 2008. This review was not completed due to an increase in requests for advice and support to public bodies on privacy and information sharing initiatives, along with a significant increase in Justice-specific access-to-information requests related to substantiating negative impacts of the residential school experience. It is anticipated this work will be advanced in the 2010/11 fiscal year, barring further increases in access-to-information requests (which take priority due to legislated, time-sensitive reporting</p>	<p>The Department of Justice has not advanced this work due to competing priorities.</p> <p>The GNWT Access and Privacy Office has experienced a 305% increase in Justice ATIPP requests since 2008. In 2010, the Department received additional resource funding to help meet the significant increase in operational pressures.</p> <p>During this time frame the GNWT Access and Privacy Office has focused on other priorities that strengthen capacity of the GNWT in meeting its access and privacy obligations, as indicated in past GNWT responses to Standing Committee.</p> <p>The Department will return to this work following the completion of the comprehensive review, which has been identified as a priority of this assembly.</p>	<ul style="list-style-type: none"> Work will be advanced following the comprehensive review of the ATIPP Act.

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
<p><u>Recommendation 4</u></p> <p><i>The Standing Committee on Government Operations recommends the Access to Information and Protection of Privacy Act be amended to extend the period of time in which applicants may ask that a decision on a Request for Information be reviewed by the Information and Privacy Commissioner.</i></p> <p><i>(Committee Report 1-16(4); page 3)</i></p>	<p>requirements).</p> <p>The <i>ATIPP Act</i> (Section 51c) provides for service of documents in a manner that allows for verification of the date of delivery. The Department of Justice will commit to review time frames related to requests for reviews that have occurred since 2006, in order to assess if current time frame provisions under the Act are adequate or require amendments. This evaluation will include an examination of timelines related to when applicants are notified of decisions, when applicants notify the Information and Privacy Commissioner of a request for appeal, and when Departments are notified of the appeal.</p>	<p>This was discussed at the June 2010 Access and Privacy Administration Committee. Access and Privacy Coordinators were informed the purpose of this review was to assess the effectiveness of the current review time frame.</p> <p>The following information was requested:</p> <ul style="list-style-type: none"> • Date when applicant was notified of the public body's decision; • Date when applicant notified the Information and Privacy Commissioner of a request for appeal; • Date when the public body was notified of an appeal. <p>This issue was raised with the Committee on subsequent meetings; however the Office has not received the required information from all affected public bodies. This is due in part, to staffing changes and confusion on the number of reviews public bodies have received.</p>	<ul style="list-style-type: none"> • The GNWT Access and Privacy Office will address amending the extension of the review appeal period during the comprehensive review of the ATIPP Act.
<p><u>Recommendation 5</u></p> <p><i>The Standing Committee on Government Operations recommends that the GNWT develop policies to address electronic records and their relationship to ATIPP, and that the GNWT provide training to employees on this issue.</i></p> <p><i>(Committee Report 1-16(4); page 3)</i></p>	<p><i>The GNWT has three policies specific to electronic information:</i></p> <ol style="list-style-type: none"> 1. <i>the Management of Electronic Information, 6003.00.20;</i> 2. <i>the Email Use Policy, 6003.10.11; and</i> 3. <i>the Electronic Information Security Policy 6003.00.26.</i> <p><i>The Management of Electronic Information Policy provides overarching direction on information management in the electronic environment, including email. It assigns responsibility for management to the department that creates or receives the</i></p>	<p>The three policies identified to Standing Committee and the <i>Guidelines for Managing Electronic Mail Messages</i> are the current policies and guidelines addressing electronic records and their relationship to ATIPP.</p> <p>As noted above, the OCIO is reviewing the <i>Electronic Information Security Policy 6003.00.26</i>.</p> <p>The GNWT Access and Privacy Office delivers ATIPP training for GNWT employees, which</p>	<ul style="list-style-type: none"> • The <i>Electronic Information Security Policy 6003.00.26</i> and its supporting guidelines will be reviewed as resources become available. • The GNWT Access and Privacy Office have introductory and advanced access and privacy training courses scheduled

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
	<p><i>information. The policy covers factors such as the classification and destruction of electronic information, and the requirement for departments to manage their electronic information in compliance with this policy as well as the ATIPP Act, the Archives Act, the Financial Administration Act and all other GNWT legislation.</i></p> <p><i>The Email Use Policy provides specific guidance on the use of GNWT email, explains the impact it has on shared technology resources, and provides clarity on related privacy, security and records management matters. Users of GNWT email are notified email is considered a government record and can be accessed under the ATIPP Act.</i></p> <p><i>In conjunction with the above two policies, guidelines were developed for employees on managing email. The Guidelines for Managing Electronic Mail Messages gives direction on effective and secure management of email. The policy and the guidelines are available on the Human Resources and Public Works & Services websites. Additionally, Records Management of Public Works & Services developed a Managing Electronic Records Course for employees. The course takes an in-depth look at the management of electronic records and how GNWT legislation, policy and guidelines apply to electronic records. The course has been routinely offered to GNWT employees since December 2004.</i></p> <p><i>The third policy, Electronic Information Security Policy, provides direction on implementation of information security standards, guidelines and procedures. It creates baseline requirements and responsibilities for the secure use of electronic information, information systems and technologies. As noted in the GNWT's response to Recommendation 2, the policy and guidelines are currently under review with the interdepartmental Security Officers Committee. The intent of the review is to update the policy and guidelines to address emerging technologies and standards. An updated policy is anticipated to be completed by summer 2010.</i></p>	<p>includes reference to both paper and electronic records in training modules, and course materials.</p> <p>The Managing Electronic Records Course developed by Records Management of Public Works & Services (PWS) was implemented in 2004 and addresses the management of electronic records and how GNWT legislation, policy and guidelines apply to electronic records. This course was routinely offered between 2004 and 2009 however Public Works and Services has not offered the course since 2009, due to staffing constraints and conflicting demands for limited resources.</p>	<p>for 2012-2013.</p> <ul style="list-style-type: none"> • PWS will update the course and offer training as resources become available.

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
<p><u>Requested Update on a Recommendation from the 15th Legislative Assembly's Standing Committee on Accountability and Oversight Report – Re: Municipalities</u></p> <p><i>The Committee has been informed that the Department of Municipal and Community Affairs will present a discussion paper to various territorial associations, municipal governments and the general public in the next two to three years. The Committee continues to support working toward this legislative initiative in a timely fashion and will monitor progress in the coming months.</i></p> <p><i>(Committee Report 1-16(4); page 4)</i></p>	<p><i>The Department of Municipal and Community Affairs (MACA) supports the Standing Committee's recommendation to conclude the work started in consultation with the Northwest Territories Association of Communities and the Department of Justice to explore options that may include legislative solutions to address access and privacy considerations.</i></p> <p><i>Further analysis and broader consultation on the identified options has not been advanced due to other priorities. Currently, MACA is dedicating available resources to improving capacity to ensure community governments are capable of sustaining adequate programs and services for residents, and implementing their expanded authorities and accountabilities.</i></p> <p><i>MACA anticipates advancing this work in the next two to three business cycles when resources become available. The Department will work closely with its partners to identify viable options that represent the collective interests of the GNWT, municipal governments and residents. MACA will be working with its partners over the coming months to develop a work plan.</i></p>	<p>The status of this work will be included in the GNWT response to the <i>Standing Committee on Government Operations Report 1-17(3) on the Review of the Information and Privacy Commissioner of the Northwest Territories.</i></p>	<p>Not Applicable</p>
<p>Report on the Review of the 2008-2009 Annual Report of the Information and Privacy Commissioner of the NWT Tabled November 1, 2010 GNWT Response Tabled February 28, 2011</p>			
<p><u>Recommendation 1</u></p> <p><i>The Standing Committee on Government Operations recommends that the Government of the Northwest Territories place a full review of the Access to Information and Protection of Privacy Act on its agenda.</i></p> <p><i>(Committee Report 5-16(5); page 2)</i></p>	<p><i>The GNWT supports in principle, the need for effective review mechanisms. The GNWT's commitment to providing open, accessible and accountable government to the people of the Northwest Territories is evidenced by the numerous amendments to the ATIPP legislation, policies, guidelines and training that have taken place since the Act came into force in 1996.</i></p> <p><i>The current review mechanism to address access and privacy issues identified by the Information and Privacy Commissioner is through the Legislative Assembly by means of the Standing Committee's review of the Commissioner's annual reports. This</i></p>	<p>The GNWT will undertake a comprehensive review of the ATIPP Act, including an examination of the role and powers of the Information and Privacy Commissioner. This work and other actions in response to past commitments (as identified in this progress report) will be the focus of the GNWT Access and Privacy Office during the 17th Assembly.</p> <p>The GNWT Access and Privacy Office has focused on a number of best practises initiatives that strengthen the capacity of the GNWT in meeting its access and privacy obligations.</p>	<p>The GNWT will develop a review framework in 2013-14, with the goal of completing the review before the end of the 17th Assembly. Completion of the review is dependent on the availability of resources and timing considerations.</p> <p>Status of GNWT Access and Privacy Office initiatives:</p>

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
	<p><i>review mechanism has been in place since the late 1990s, and has enabled the GNWT to respond to recommendations made by the Legislative Assembly on a wide range of issues identified by the Commissioner, including those focused on information and communication technologies.</i></p> <p><i>Additionally, the executive branch of government has processes and initiatives to improve the GNWT's capacity and performance. The Minister of Justice is responsible for the administration of the ATIPP Act and takes a proactive approach in both (1) promoting access to information created and received by the GNWT and (2) protecting individual privacy rights related to that information. The Minister demonstrates this commitment by a number of best practice initiatives, including:</i></p> <ul style="list-style-type: none"> <i>• Creation of an Access and Privacy Administration Committee comprised of access and privacy coordinators from all public bodies, whose mandate is to communicate the importance of access and privacy guidelines, policies and standards to all public bodies;</i> <i>• Creation of an annual activity report on the administration of the Act which will include information relating to access and privacy activities for GNWT departments;</i> <i>• Routine updates to the GNWT Access and Privacy Office web information (on the Justice website) which indicates the role of the Office and its services to both the public and the government;</i> <i>• Development and coordination of access and privacy training specific to coordinators, as well as customized for training for program areas or GNWT boards and agencies;</i> <i>• Development of an on-line training session, which is anticipated to be launched on the GNWT Access and Privacy Office web pages by spring 2011; and</i> <i>• GNWT participation at a national subcommittee made up of representatives from all jurisdictions. This committee takes a leadership and coordination role in matters related to access</i> 	<ul style="list-style-type: none"> • The Access and Privacy Administration Committee was formed in June 2010. The Committee is comprised of Access and Privacy Coordinators from all public bodies and committee meetings are held quarterly. • The implementation of an Annual Activity Report on the administration of the Act has not advanced due to competing priorities of the GNWT Access and Privacy Office. However, the Office continues to collect statistics relating to the report and anticipates moving forward on this initiative as resources become available. • The Department of Justice routinely updates the GNWT Access and Privacy Office web page. This includes yearly updates to the GNWT Access and Privacy Directory, as well as updates to training initiatives and Access and Privacy Coordinator listings as required. • The GNWT Access and Privacy Office updated all ATIPP course modules and training resources in 2010. The Office also developed customized training for program areas or GNWT boards and agencies, on request. • The GNWT Access and Privacy Office developed an online Access and Privacy training course for GNWT employees. However, this initiative has not advanced due to resource constraints. • The Senior Policy Advisor, Information and Privacy is the GNWT representative on the Public Service Chief Information Office Council – Privacy Subcommittee since 2006. This committee takes a leadership and coordination role in matters related to access to information and privacy 	<ul style="list-style-type: none"> • The Access and Privacy Administration Committee next meeting is scheduled for September 27, 2012. • The Annual Activity Report will advance as resources become available. • Routine updates to the Department of Justice, GNWT Access and Privacy Office website continue to take place. • GNWT Access and Privacy Training course are regularly noted on the GNWT Training Calendar and the GNWT Access and Privacy Website. Customized training courses for departments or program areas, have taken place and more are scheduled for Fall 2012. • The Department of Justice Online Access and Privacy training course for employees will advance as resources become available. • The GNWT continues to participate in the National Public Service Chief Information Council's Privacy Subcommittee. The next

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
	<p><i>to information and privacy protection across Canada, and develops tools and best practises that governments can adapt to improve their capacity.</i></p> <p><i>The Minister's and Department's activities along with the Legislative Assembly's review mechanisms collectively ensure that the ATIPP Act, policies and guidelines remain current and relevant to address the emerging trends and issues identified by the Information and Privacy Commissioner.</i></p>	<p>protection across Canada, and develops tools and best practises that governments can adapt to improve their capacity.</p>	<p>meeting is tentatively scheduled for February 2013.</p>
<p><u>Recommendation 2</u></p> <p><i>The Standing Committee on Government Operations recommends that when a reorganization, amalgamation or formation of any public body is planned, matters concerning privacy issues should be considered and addressed at the organizational design stage.</i></p> <p>(Committee Report 5-16(5); page 2)</p>	<p>The GNWT recognizes the benefits of a proactive approach in reviewing privacy considerations in all aspects of government work. This includes reviewing privacy implications at the organizational design stage as well as when considering new or modified programs, information systems or administrative practises or legislation.</p> <p>The GNWT Access and Privacy Office has developed a variety of privacy tools to aid public bodies in establishing practises and procedures that take into consideration the legislative requirements of the <i>ATIPP Act</i>. Two tools have been developed to identify privacy issues in the design stage:</p> <ol style="list-style-type: none"> 1. A <u>Preliminary Project Screening Tool</u> will assess new projects/programs or where changes are being proposed to existing projects involving the use of personal information. This enables public bodies to determine whether a formal Privacy Impact Assessment is required. 2. <u>Two Privacy Impact Assessment Modules</u> were developed in 2008 and recently updated. The Privacy Risk Assessment Module is designed as a project scoping tool to determine to what extent the project under consideration is "privacy intrusive", and what level of effort is required in the privacy impact assessment to ensure that identified risks are appropriately mitigated. The Privacy Analysis Module was designed to assist employees in conducting a more in-depth privacy analysis to ensure public bodies are in compliance 	<p>As noted in the original response, the GNWT Access and Privacy Office developed a variety of privacy tools to aid public bodies in establishing privacy practices. The privacy tools noted in the original response has been distributed to public bodies, through the GNWT Access and Privacy Administration Committee and the Information Technology Advisory Committee.</p> <p>The Office, in collaboration with the OCIO are currently working on the following privacy initiatives:</p> <ul style="list-style-type: none"> • Development and implementation of GNWT-wide information incident protocols in consultation with the OCIO; • Development of a GNWT-wide privacy policy and implementation framework, in consultation with the OCIO and the Department of Human Resources. <p>These projects have been noted in the Departments of Justice and Finance Business Plans.</p>	<ul style="list-style-type: none"> • The draft Information Incident Protocol was shared with the Information Technology Advisory Committee and the Access and Privacy Administration Committee in July 2012. • The GNWT Privacy Policy and implementation framework is anticipated to be completed in 2013.

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
	<p>with government policy and core privacy principles for projects involving the use of personal information.</p> <p>The GNWT Access and Privacy Office will continue to develop tools and guidelines to aid public bodies to identify privacy considerations at the earliest possible stage.</p>		
<p><u>Recommendation 3</u></p> <p><i>The Standing Committee on Government Operations recommends that the Government of the Northwest Territories enact legislation that would make municipalities subject to access and privacy legislation, would define accountability levels, and would create practical rules regarding the gathering, use and disclosure of personal information about individuals by municipalities.</i></p> <p>Committee Report 5-16(5); page 2)</p>	<p>The Department of Municipal and Community Affairs (MACA) agrees and supports the recommendation in principle. Implementation issues identified by community governments as stated in previous GNWT responses to Standing Committees relating to capacity, costs and training continue to be a factor in the delay to moving forward with the recommendation to enact legislation that would make municipalities subject to access and privacy legislation.</p> <p>In the GNWT's response to the 2006-2007 and 2007-2008 Standing Committee report, MACA anticipated advancing this work in the next two to three business cycles when resources become available, and noted it would work with its partners to identify options and develop a work plan. However, no work was advanced on this initiative given other workload pressures of the Department and of community governments.</p> <p>MACA recognizes that this is an outstanding recommendation and acknowledges the importance of the issue identified by the Information and Privacy Commissioner. The Department will continue to monitor the capacity of community governments, and examine the broad range of options that may be available, and could consider moving forward on the recommendation during the 17th Legislative Assembly if sufficient resources are available.</p>	<p>The status of this work will be included in the GNWT response to the <i>Standing Committee on Government Operations Report 1-17(3) on the Review of the Information and Privacy Commissioner of the Northwest Territories.</i></p>	<p>Not Applicable</p>

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
<p><u>Recommendation 4</u> <i>The Standing Committee on Government Operations recommends that the Government of the Northwest Territories ensure that:</i></p> <ul style="list-style-type: none"> <i>The same good records management practices that are applied to paper records are applied to e-mail communications; and</i> <i>Employees receive formal training and informal coaching on managing electronic records.</i> <p>2008-2009 Committee Report 5-16(5); page 3)</p>	<p>The GNWT agrees and has policies, guidelines and training specific to the management of electronic information.</p> <p>The <i>Management of Electronic Information Policy</i> provides overarching direction on information management in the electronic environment, including email. It assigns responsibility for management to the department that creates or receives the information.</p> <p>The <i>Email Use Policy</i> provides specific guidance on the use of GNWT email, explains the impact it has on shared technology resources, and provides clarity on related privacy, security and records management matters.</p> <p>The <i>Electronic Information Security Policy</i> provides direction on implementation of information security standards, guidelines and procedures. It creates baseline requirements and responsibilities for the secure use of electronic information, information systems and technologies. As noted in the GNWT response to the 2006-2007 and 2007-2008 Standing Committee report, this policy is scheduled to be updated to address emerging technologies and standards. The Department of Finance (Chief Information Office) indicates the review of this policy and the <i>Email Use Policy</i> will continue as resources become available.</p> <p>In conjunction with the above policies, guidelines were developed for employees on managing email. The <i>Guidelines for Managing Electronic Mail Messages</i> gives direction on effective and secure management of email. Additionally, the Department of Public Works (PWS Records Management) has developed a Managing Electronic Records Course for GNWT employees which had been routinely running since December 2004.</p> <p>The GNWT is also developing a management and employee guide to privacy, access, security, retention, disposal and overall management of information in government and public bodies in the NWT. The Departments of Justice (Access and Privacy</p>	<p>Implementation of a GNWT management and employee guide to privacy, access, security, records retention, disposal and overall management of information in government has been delayed due to competing priorities, however this item has been identified in the Department of Justice Business Plan.</p>	<ul style="list-style-type: none"> The <i>Electronic Information Security Policy</i> and its supporting guidelines will be reviewed as resources become available. The GNWT Employee Guide is anticipated to be completed by 2013.

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
	Office), Finance (Chief Information Office), PWS (Records Management) and Human Resources are collaborating on this project. This guide is anticipated to be completed in spring 2011.		
<p><u>Recommendation 5</u></p> <p><i>The Standing Committee on Government Operations recommends that the GNWT give consideration:</i></p> <ul style="list-style-type: none"> <i>To educating elementary and secondary students about the risks associated with online activities; and</i> <i>To providing specific information in school curricula about these risks and the precautions that should be taken in order for youth to reduce them.</i> <p>Committee Report 5-16(5); page 3)</p>	<p>The GNWT recognizes the importance of educating students and teachers about both the risks and the benefits that can be gained through responsible online activities.</p> <p>The Department of Education, Culture and Employment (ECE) has a variety of resources currently available, such as a series of web awareness workshops for teachers and online tutorials, regarding safe online practices for students. ECE is developing a curriculum for elementary and secondary students to address the use of information and communication technology. The overall goal of this curriculum is to educate students to be critical and creative in their use of information and communication technologies, while also protecting themselves from the risks associated with online activities. The curriculum is currently in its pilot stage and is anticipated to be formally implemented in 2012.</p> <p>Notwithstanding these activities, it is important to recognize that this recommendation reflects a broader public interest regarding safe online activities that is not regulated by the <i>ATIPP Act</i>.</p>	<p>The status of this work will be included in the GNWT response to the <i>Standing Committee on Government Operations Report 1-17(3) on the Review of the Information and Privacy Commissioner of the Northwest Territories.</i></p>	<p>Not Applicable</p>
<p><i>Report on the Review of the 2009-2010 Annual Report of the Information and Privacy Commissioner of the NWT</i> <i>Tabled May 17, 2011</i> GNWT Response tabled August 17, 2011</p>			
<p><u>Recommendation 1</u></p> <p><i>The Standing Committee on Government Operations recommends that the Government of the Northwest Territories review the fee schedule to the Access to</i></p>	<p>Section 5(3) of the <i>ATIPP Act</i> and Schedule 2 of the regulations establish the maximum fees that may be charged for processing a “general” access request, and the fees that may be charged for a “personal” access request where the applicant is accessing his or her own personal information.</p>	<p>The GNWT committed to undertake a jurisdictional review of general access to information fees in order to assess if the NWT’s current fee structure is consistent with other jurisdictions.</p> <p>The NWT is:</p> <ul style="list-style-type: none"> 1 out of 4 jurisdictions that require an initial 	<ul style="list-style-type: none"> Jurisdictional comparison of Access to Information fees completed. Sections of the <i>ATIPP Policy and Guidelines Manual</i> including all appendices and

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
<p><i>Information and Protection of Privacy Act to ensure that it is clearly worded and does not place an undue cost on persons requesting access to information.</i></p> <p>(Committee Report 5-16(6); page 2)</p>	<p>In the case of a request for an applicant's own personal information, an applicant only pays copying fees, and only when those fees exceed \$25, in accordance with the rate established in the fee schedule. Additionally, the Act provides limited situations where fees can be reduced or waived entirely if an applicant cannot afford to pay or there are other reasons justifying excusing the fee, or if the record relates to a matter of public interest.</p> <p>For applicants requesting access to general information, the ATIPP regulations set out the maximum fees that may be charged for processing a request. This fee structure allows public bodies to charge modest fees to help offset the cost of providing applicants with access to records.</p> <p>The GNWT appreciates the need for clarity and consistency in applying fees and will bring this issue forward by the GNWT Access and Privacy Office to the Access and Privacy Administration Committee for review. The GNWT further commits to undertake a jurisdictional comparison of access to information fees to assess if the current fee structure is in keeping with other governments.</p>	<p>application fee of \$25.00 for general requests. All other jurisdictions charge less or no fee charges;</p> <ul style="list-style-type: none"> • 1 of 11 jurisdictions that charge between \$27.00-\$30.00 dollars an hour for search and preparation for general requests. The other two jurisdictions charge less; • 1 of 8 jurisdictions that charges 25 cents per page for normal copying fees. Four other jurisdictions charge less, and one charges more; • 1 of 9 jurisdictions that charges for the "actual" shipping costs for delivery of documents. The other 4 jurisdictions do not charge for regular shipping. <p>The GNWT will assess the fee structure further during the course of the comprehensive review of the Act.</p> <p>The GNWT Access and Privacy Office has revised the fee section of the ATIPP Policy and Guidelines Manual. The updated section clarifies the application of fees, fee estimates or fee waivers. The updated section along with its supporting model letters was discussed at the February 2012 Access and Privacy Administration Committee meeting.</p>	<p>model letters continue to be updated and distributed as required.</p> <ul style="list-style-type: none"> • A new edition of the ATIPP Policy and Guidelines Manual will be completed following the comprehensive review of the ATIPP Act. <p>The GNWT considers its response to this recommendation completed.</p>
<p><u>Recommendation 2</u></p> <p><i>The Standing Committee on Government Operations recommends that the Government of the Northwest Territories institute requirements for proactive disclosure of employee bonuses and the salaries of senior employees, or bring forward</i></p>	<p>The ATIPP Act is structured to provide a balance between the public's right to access information held by government, and an individual's right to expect privacy protections regarding their information held by government.</p> <p>The Act establishes a mandatory exception to disclosure of personal information if the disclosure may result in an unreasonable invasion of an individual's privacy (Section 23(2)). However, the Act further clarifies it is <u>not</u> an unreasonable invasion of an individual's personal privacy to disclose</p>	<p>The GNWT is committed to providing the public with information about public service salaries while ensuring the privacy protections for GNWT employees are maintained.</p> <p>The GNWT has posted salary range information for GNWT employees on the Department of Human Resources website and is exploring options for consideration of proactive disclosure of bonus ranges. The Department's review of the merits of a</p>	<ul style="list-style-type: none"> • The review of the merits of a legislated approach for proactive disclosure is ongoing.

SCOGO Recommendation	Original Government Response	Status of Work	Next Steps
<p><i>legislation to this effect if legislation is necessary.</i></p> <p>(Committee Report 5-16(6); page 3)</p>	<p>information relating to an employee's job classification, salary range, discretionary benefits or employment responsibilities (Section 23 (4e)).</p> <p>There is a distinction between disclosures of "salary range" information for an employment position, and the "actual salaries" of senior employees. A salary range means a variety of fixed regular payments that are associated with an employment position, whereas an employee's individual salary is considered their personal information.</p> <p>The current mechanism for responding to requests for disclosures of employee bonuses and salaries is to process the requests under the ATIPP Act. Requests for disclosure are addressed on a case-by-case basis according to the information involved and the scope of the request. Disclosing the name and actual salary of employees under the current legislation is considered, in most instances, an unreasonable invasion of the individual's privacy.</p> <p>Proactive disclosures of employee salary and bonuses would require amendments to the current legislative framework. At this time, the GNWT does not support changes to the existing mechanism to access this type of information; however, the Department of Human Resources will review the merits of a legislated approach and the impacts it may have on the GNWT public service. Timelines for this work will be dependent on the availability of resources and the legislative priorities of the new government.</p>	<p>legislated approach for proactive disclosure is still ongoing.</p>	