OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Access Controls

Royal Newfoundland Constabulary

January 13, 2023

Table of Contents

EXECUTIVE SUMMARY

The *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015)* authorizes audits of public bodies by the Office of the Information and Privacy Commissioner (OIPC). The OIPC's Audit and Compliance Program addresses matters such as evaluating the adequacy of public body safeguards to protect personal information and compliance with the *Act*.
Citizens expect the OIPC, as the oversight body, to:

- assess compliance with the law;
- advocate for best practice; and
- assist public bodies in establishing effective privacy management programs.

This is the fifth comprehensive audit completed by the OIPC.

The RNC is the provincial police force in Newfoundland and Labrador, providing services to 15 communities and serving a population of approximately 214,000 people. In addition to responsibilities for traffic safety on highways, waterways and trails, the RNC provides investigative services, such as the child exploitation unit, computer forensics, crime stoppers, drug investigation unit, major crimes unit, missing persons coordinator, polygraph, surveillance and intelligence gathering and analysis.

The purpose of this Report is to examine the access controls in place in specific RNC systems. As electronic access controls will not prevent an authorized user from unauthorized access, use or disclosure of the information, other safeguards are required to ensure users understand why they have access, what they are allowed to do with this access and any consequence of non-compliance. As such, the audit also examines associated policies, procedures and training.

While OIPC has issued audit reports in the past, this Report diverts from past practice. There is risk in publishing specific details of RNC systems and highlighting details of areas for improvement. Prior to finalizing this Report, OIPC presented RNC with detailed factual information upon which the following summary and recommendations are based. The RNC had the opportunity to provide additional information and correct any misunderstandings. This

updated information is what is reflected in this Report. Again, although the Report provides limited information specific to RNC systems, readers can be assured that OIPC conducted a thorough review of the systems subject to this audit.

INTRODUCTION

The Office of the Information and Privacy Commissioner of Newfoundland and Labrador (OIPC) provides independent oversight of the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*) and the *Personal Health Information Act* (*PHIA*), as well as related regulations. The OIPC's Audit and Compliance Program includes evaluating the adequacy of public body safeguards to protect personal information and comply with *ATIPPA, 2015*. Audits are conducted under the authority of section 95(1)(b) and section 95(3) of *ATIPPA, 2015*. Section 95(1)(b) empowers the Commissioner to monitor and audit the practices and procedures employed by public bodies in carrying out their responsibilities and duties under this *Act*. Section 95(3) extends the Commissioner's investigative powers established elsewhere in Part IV to other activities, including audit.

Citizens expect the OIPC, as the oversight body, to assess the level of compliance with the law, to advocate for best practice and to assist public bodies in establishing effective privacy management programs.

The mandate of the Royal Newfoundland Constabulary (RNC), under the authority of the *Royal Newfoundland Constabulary Act, 1992*, is to provide police services and to maintain traffic and other patrols in designated areas of the province; these include the northeast Avalon, Corner Brook and Western Labrador. Through their duties, employees of the RNC collect and access large amounts of personal information.

There are a number of reasons why the OIPC has selected the RNC for audit. The RNC holds or can access databases with information on the vast majority of residents of the island and has access to national databases held by other law enforcement entities.

As indicated in the RNC's 2021 Activity Report, there are approximately 404 police officers and 101 civilian staff working out of offices on the Northeast Avalon, Corner Brook and Labrador West; there is potential for a large number of people to have access to information. In addition to the sheer volume of information held and accessed by the RNC, our Office has received privacy complaints and breach reports involving the RNC. During the resolution

process of these complaints, the RNC has made commitments to make changes and improve information handling practices. In particular, Report P-2015-002 contained a number of recommendations pertinent to this audit, establishing expectations regarding role-based access, privacy training, oaths of confidentiality, a Privacy Impact Assessment (PIA) of the Integrated Constabulary Automated Network (ICAN) system, policies and procedures and an auditing program.

In 2017 prior to the launch of this audit, another employee was charged with a similar offence. That individual pleaded guilty and received a fine of $1000. Since this audit was launched, two employees of the RNC were charged with offences contrary to section 115 of *ATIPPA, 2015*. The charges related to inappropriately accessing personal information without lawful authority while in the employ of the RNC. One employee plead guilty and received an absolute discharge. The case involving the other employee went to trial, and that individual was found not guilty of the charge.

AUDIT OBJECTIVES

The key objectives of this project are to:

- examine access to personal information in various databases held or accessed by RNC staff;
- examine training provided to staff regarding acceptable use of access privileges;
- review the extent to which RNC policies and practices reflect legislative requirements;
- identify any risk factors in the protection of personal information; and
- make recommendations to strengthen RNC policy and practice.

The lines of inquiry for this audit comprised whether the RNC:

- has reasonable safeguards in place regarding electronic access controls as required by section 64 of *ATIPPA, 2015*;
- has met its obligations under *ATIPPA, 2015* relating to policies and practices, training and acceptable system use; and

- has an understanding of the personal information contained in each system subject to this audit.

AUDIT FOCUS

This audit focuses on the electronic access controls, acceptable use and staff training on the electronic systems to which the RNC have access as part of compliance with section 64 of *ATIPPA, 2015*, which states in part:

> *64.(1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that*
>
> *(a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;*
> *(b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and*
> *(c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.*

OIPC is frequently asked what constitutes reasonable and discussed this in detail in our first audit, which examined physical safeguards.

In Report P-2008-002, this Office identified four criteria it would consider when determining if reasonable safeguards were in place, including the foreseeability of the privacy breach, the seriousness of potential harm, the cost of preventative measures and the relevant standards of practice. While this Report was issued after a privacy breach, the same criteria should be used in a proactive fashion to better protect against a breach occurring.

There are physical, administrative and technical forms of safeguards. Technical safeguards are the technologies (communication systems, hardware, software, etc.) and the policy and procedures for its use that protect electronic personal information. These safeguards monitor, control, and address access controls, data in motion, and data at rest requirements. Public bodies should implement accompanying policies and procedures for IT systems that store personal information to ensure only authorized users are able to access such information. There are many best practices and considerations when examining access. In 2020, Securing Personal Information: Self-Assessment Tool for Public Bodies and Organizations was

published jointly by the OIPC British Columbia, OIPC Alberta and the Office of the Privacy Commissioner of Canada. Considerations under access include:

General

12.1 Are there policies in place that require enhanced (multi-factor) authentication for privileged accounts?

12.2 Where appropriate, does the network access policy include a requirement that each user, at login, is informed of the date and time of the last valid logon and any subsequent failed logon attempts?

12.3 Are controls in place to detect any discrepancies in login attempts?

User registration, access and approval

12.4 Is a formal user registration and deregistration process in place?

12.5 Does the registration process include verification of user identity, verification and approval of access privileges, audit processes and actions to ensure access is not granted until approved?

12.6 Is each user of a system that processes personal information uniquely identified (no shared/generic accounts)?

12.7 Is the identification of the authorizer retained in the approval transaction record?

12.8 Is a current, accurate inventory of user accounts maintained and is it reviewed on a regular basis to identify dormant, fictitious or unused accounts?

Roles

12.9 Is access control based on defined roles in your organization?

12.10 Are access privileges limited to the least amount of personal information required to carry out the role?

12.11 Is a monitoring process in place to oversee, manage and review user access rights and roles at regular intervals?

12.12 Is there a clearly defined separation or segregation of duties (for example someone who initiates an event cannot authorize it) in the access management process?

12.13 Has the role been defined for managing access control on the various systems and platforms in the network?

12.14 Is a privacy officer role defined for all systems containing personal information that includes access control, data integrity, as well as backup and recovery?

12.15 Are roles and access rights for partners and third-party organizations (such as consultants, off-site storage) clearly defined?

12.16 Are access privileges allocated, modified or removed only after formal authorization?

Authentication

User authentication is the mechanism by which user identities are confirmed prior to granting access to a system.

12.17 Are the authentication mechanisms that are implemented commensurate with the sensitivity of the information and the associated risks (that is the more sensitive the information, the more robust the authentication mechanism)?

12.18 Are authentication codes or passwords generated, distributed and managed to maintain confidentiality and prevent unauthorized use?

12.19 Where authentication is based on username and password, are effective policies or controls in place to ensure robust passwords are used

AUDIT SCOPE

On September 20, 2017, this Office communicated the intent to launch an audit of the RNC and requested a launch meeting. To assist in preparing for the meeting, the OIPC requested a list of all systems to which staff have access, including a brief description of the system, the identified purpose for access, the type of information contained within the system, an example of a common use of the system and an indication of the number of staff with access.

The Office corresponded and met with representatives of the RNC during Fall 2017 to identify the systems that would be in scope for the audit. The systems described as the main, primary systems in use by the RNC attending the meeting are within scope. These include:

- Integrated Constabulary Automated Network (ICAN)
- Mobile Report Entry System (MRE)/Mobile Data Terminals (MDT)
- RNC MOBL

Also in scope is Closed-Circuit Television (CCTV). For the purpose of this audit, the area of interest is the CCTV in use in public areas, such as George Street. The audit will not examine the use of CCTV in and around RNC facilities.

There are a number of electronic systems that have been determined to be out of scope. These are either external systems to which the RNC have access, systems that contain little to no personal information and/or systems that have low numbers of individuals with access;

for example, federal policing systems, records management systems, training dataset, etc. Further, while the ICAN Report Warehouse was initially determined to be within scope, the RNC ceased using it during the audit process. As such, it is not examined as part of this Report. The audit formally launched in February 2018, once the final list of systems in scope was established.

SYSTEM DESCRIPTIONS

The RNC systems that fall within scope of this audit contain a large volume of information, some sensitive, on a large number of individuals.

INTEGRATED CONSTABULARY AUTOMATED NETWORK (ICAN)

The Integrated Constabulary Automated Network (ICAN) is a computerized information management system that houses the operational police files of the RNC; all electronic access to RNC file data is performed through the ICAN system. The system allows officers to manage day-to-day policing operations, including tracking dispatch information and filing completed police reports.

ICAN does not just hold personal information on convicted and suspected criminals, it also houses personal information related to victims and witnesses. The RNC's 2021 Activity Report indicated that officers responded to 69,485 calls for service and generated 35,561 operational files; the ICAN system holds a large quantity of personal information. The information can include an individual's criminal history, basic contact information, and other personal information captured as part of police/legal proceedings or reports. It also contains attachments such as photos, videos, court documents, PDFs or emails and narrative text documentation.

ICAN is designed to support the RNC's operation and comprises three systems: Computer Aided Dispatch (CAD), Records Management System (RMS), and the Mobile Work Station (the collective name for the Mobile Data Terminal (MDT)/Mobile Report Entry (MRE)). Each System comprises a number of subsystems.

COMPUTER AIDED DISPATCH (CAD)

The Computer Aided Dispatch (CAD) system is used primarily by Communication Center staff when calls for police assistance are received. Addresses are pre-loaded into CAD, using information provided by covered municipalities.

CAD is used to collect caller information and initial details of an incident. If the call requires police response, an officer is dispatched and the call for service is sent to Mobile Data Terminals (MDTs) located in police vehicles. If the call is deemed to be non-reportable, it is concluded and brief remarks or notes are often added by the responding officer. No further details are included on the investigation itself in the CAD system. However, if the call for service is deemed reportable, it is prefilled into MRE and a police operational file is created. The CAD system creates tracking data, such as assigning a file number, details on unit status, and monitoring threshold times and provides much of the call information to the Records Management System (RMS).

Records Management System (RMS)

The Records Management System (RMS) is the central database used to store and organize file information. RMS supports data entry, management and access to information related to police business, including complaints, general occurrences and tickets. The information contained in the system includes names of individuals (both suspects and victims), vehicle details, and general details surrounding events.

The RNC must maintain records of information relevant to law enforcement activities and public safety in their community (e.g. information related to violation tickets; charges; arrests; evidence; ongoing investigations; and property). RMS classifies information based upon Uniform Crime Reporting (UCR), a system developed by the Canadian Center of Justice Statistics (CCJS). The data includes all categories of crime and traffic incidents occurring within a police jurisdiction.

Crime scene pictures or surveillance information is not allowed on RMS; the information contained in RMS tends to be citizen submitted information. Records that can be attached include court orders and known offenders.

RMS has an internal messaging system known as Vmail that can be accessed on MDT. Vmail does not automatically appear on MDT when users login; it must be actively retrieved from the users RMS mailbox; only new messages will appear on MDT. Vmail allows users to send messages to individuals and user handles; user handles would be a particular security group, such as all those involved in domestic violence.

Mobile Work Station (MWS)

The Mobile Workstations (MWS) are located in patrol cars. A secure network is used to connect them to a closed network with limited resources. There is no connection to the internet, RNC network file storage or RNC email systems. Installed on the MWS is Mobile Data Terminal (MDT) and Mobile Report Entry (MRE). MWS also establishes access to the RNC's frontline intranet and Motor Registration Division (MRD) web known as RNC MOBL.

Mobile Data Terminal (MDT)

The Mobile Data Terminal (MDT) is an application that accepts information from, and provides information to, a dispatch center using a connection to the CAD system. The application is used to receive calls of service information, communicate with dispatch center and other MWS units. MDT is also has query function, where it can retrieve read-only information from various systems. None of the information retrieved by MDT is retained on the MWS.

Mobile Report Entry (MRE)

The Mobile Report Entry (MRE) application is a field reporting system that is capable of off-line report entry, which enables the reports to be taken as close to the source of the information as possible. The MRE helps officers record field information in an effective manner (taking advantage of the MWS), and then transfer this collected data as quickly and efficiently as possible to the main records system. In MRE, officers can enter many types of

reports (e.g., General Occurrence, Street Check, Follow Up, etc.) and then index additional records (e.g., person, vehicle, detail pages, etc.) to the report.

CLOSED CIRCUIT TELEVISION (CCTV)

The OIPC discussed CCTV with the RNC and it was clarified that the cameras surveilling public places – George Street for the most part – would be included in the audit scope. This focus is consistent with the overall approach taken for this audit, in that the focus has been on personal information related to RNC's law enforcement mandate and not RNC staff. The cameras are usually focused on preset public areas based on historical details of calls made to the RNC. The RNC indicated that footage had been used on several occasions and the cameras were installed as a deterrent. The RNC has confirmed that the system does not use any data analytics, such as facial recognition.

In 2010, a tender was issued seeking the supply, installation, configuration, testing, training and commissioning of a video surveillance management software and hardware solution for the George Street area. At the time, the identified purpose for the system was:

> *… to provide the RNC with the capability of capturing high quality video surveillance footage in support of police investigations. This system will also have the ability to monitor special events in and around George Street in real time.*

The cameras were selected to withstand the Newfoundland weather and are able to pan, tilt and zoom.

In 2010, the ATIPP Office provided a privacy impact report on the project. It made four recommendations:

1. That signage is erected in the area to inform the public of the surveillance cameras.
2. That this PPIA be revisited in 6-12 months to review and make modifications based on any issues that may arise during that time period.

3. That there are policies put into place that provides limitations on the collection, use and disclosure of personal information captured by the cameras.
4. That employees working with the information take advantage of Access and Privacy Training by the ATIPP Office, if they haven't already done so.

SAFEGUARDS

While the focus of this audit is on system access controls, a form of technical safeguard, the layers of administration and physical safeguards in place cannot be ignored. For example, the systems subject to this audit are all government assets and all are located in RNC offices, with the exception of the mobile workstation. An individual would have to get past physical safeguards, including multiple secure doors and monitored entrances, before even having an opportunity to try to gain access to an asset and then attempting to gain access to one of the systems subject to this audit. Other physical safeguards complementing technical safeguards include the fact that the majority of computers in use are CPU's and not laptops and the availability of a secure print feature, where print jobs do not start until an employee enters a code into the printer.

The RNC network is segregated from the GNL network and must be managed from within RNC facilities. Even with all the changes brought about by the public health emergency, the RNC has not allowed remote access to the operational system subject to this audit, save for the established mobile work station. Further, any authorized user coming from an external agency, such as a visiting officer from another jurisdiction, must complete the Office of the Chief Information Officer's Terms of Use Non-Government IT Asset Form, even if they are using an asset issued by their own government/employer. For example, if a member of the Ontario Provincial Police (OPP) is working with the RNC on a case and using their OPP asset, they must still complete the Terms of Use Form.

While there are laptops that can be signed out, these are not able to access the systems under audit and are mostly used by the training division when sessions are held off-site.

With these complementary safeguards in mind, the focus shifts to access controls. Access controls are important tools that determine who has access to what data and what actions they can perform. Electronic access controls should be designed to ensure that only authorized users have access to systems and to restrict actions and access to the minimum required to fulfill duties.

There are many considerations when examining access, including, but not limited to:

- Role-based access controls, which ensure employees access only information they need to do their jobs and prevents them from accessing information that doesn't pertain to them or their position.
- Timeouts, both for systems and the IT asset. Session timeout is used to determine how long a device may remain authenticated before it must perform authentication again. Timeout features help prevent unauthorized access if a user leaves an asset unattended or if a user does not log out of a program.
- Password protections, including using unique passwords that incorporate letters, numbers, and symbols. It is best practice to ensure passwords used for work are not also used for personal accounts, as compromised passwords may be linked back to the user and allow threat actors to access other information linked to the user.
- Multi-factor authentication (an additional layer of security for electronic authentication systems that allow a user to access a website/program only after providing two or more pieces of evidence relating to their identity).

During the course of this audit, RNC provided OIPC with detailed information on the safeguards in place for each system; OIPC provided RNC with factual information to confirm details were correct before developing this summary. Rather than publish details of those safeguards, which could create a risk for the RNC, OIPC has chosen to provide general commentary on strengths and areas for improvement.

ACCESS

Most RNC employees, civilian and officers, have access to the ICAN system, totaling approximately 400-450 users. While most staff have access, privileges vary from employee to employee, with access based on division, position and role. These roles are adjusted as individuals change positions. All staff with access to ICAN receive ICAN training, coordinated through the RNC Training Section, which reflects their level of privileges in the ICAN system. Remote access to the ICAN system and its subsystems is not available and all systems within the scope of this audit are accessible exclusively through RNC work assets. To ensure that information is not retained longer than necessary there is a records classification and retention schedule in place for the ICAN system, including all subsystems, as approved by the provincial records committee.

General Order 322 (Information Management and Technology) was issued on December 10, 2013. This 18 page order addresses a number of topics, including identifying some information systems by name, providing a brief description of the system and establishing who will have access, the level of access and the training that will be provided. It states, in part:

> *10.4 Integrated Constabulary Automated Network (ICAN):*
>
> *…*
>
> *c. All sworn employees of the RNC will be permitted access to ICAN. The extent of privileges will vary from employee to employee. An employee's privileges will be determined by the employee's supervisor in consultation with the ISD [Information Services Division].*

It also establishes the process for access to the various systems, stating in part:

> *3.6 The Corporate Services Division (Department of Finance) shall distribute to the OCIO, a monthly report from the payroll system outlining the status changes of employees. This list shall include employees terminated, hired or on leave of absences from their job. This information will be used to modify the employee's access privileges to network resources.*

ICAN features end user authentication and user-based access profiles. Privileges for 24 different roles are documented, including such details as a list of record types and authorities for each, including browse, query, add, update, delete and approval. In recognition of the

sensitive nature of some of the information contained in the ICAN system, it allows for the creation and maintenance of private (restricted) records, as well as query only access to a national database called CPIC (Canadian Police Information Centre), operated by the RCMP. The CPIC database has been the subject of an audit by the Office of the Privacy Commissioner of Canada.

As part of access control, both the creation and termination of accounts was examined. While it is generally unnecessary to terminate an employee's account because they are off for a few days or away on vacation, if they are suspended, laid off or otherwise terminated it is important to remove the accounts promptly. Staff changes that may impact system access, such as promotions, are managed through personnel orders.

While our Office did not conduct a comprehensive check of each and every user, we did ask for a list of individuals who had left over a 12 month time period; the reason for leaving could be both voluntarily, such as retirement or parental leave, or involuntary, such as termination. We compared the last day in the office with the last day of system access and there were no reasons for concern.

There is a low number of staff with system administrator profiles; these profiles would include the authority to override restrictions, move an invisible file from one user to another, and add additional users. Super users and administrators use two-factor authentication to access the systems; it is important to note that these super users are not able to change their own security profiles. Access safeguards are in place to ensure that regular users (everyday operators) do not have the ability to export data, although they are able to send messages internal to systems when needed.

The Office of the Chief Information Officer (OCIO) has established password standards for government assets; this standard is mirrored on many of the RNC systems subject to this audit, but not all. ICAN accounts are managed by the RNC and use the active directory.

Currently there are only four users in the RNC who can create users on the application; two of these users can view what has been added and or changed. Each of these accounts have unique authentication criteria.

The RNC has allowed access to the ICAN system by the RCMP's Canadian Firearms Program to assist in fulfilling their responsibilities under the *Firearms Act* and the RCMP's B Division, an entity that operates as a provincial police service pursuant to the *Agreement for Policing the Province Act.* Agreements are in place governing this access.

CCTV Access to Footage

Surveillance cameras complement ongoing police presence on George Street. A small number of RNC staff have access to the footage, which is stored for a limited time and then overwritten. There is an established process when seeking access to footage involving an application form that must be approved by a supervisor. The form collects identification details of the officer, seeks a reason for the access, and collects information about the incident, such as location, date and details about the footage. The remainder of the form contains details about the information released or the reason why the request was returned.

IT Support

In addition to having appropriate safeguards in place, public bodies should engage the services of specialists who can assist in supporting technical safeguards, and who possess knowledge of software, hardware, and cybersecurity issues, and how to troubleshoot when issues arise.

The ICAN system (including RMS, MRE, and MDT) receives hardware support from the OCIO, and software support from the vendor. All other systems within the scope of this audit are supported by OCIO and the RNC.

The RNC is subject to the policies, procedures, and best practices established by the OCIO. The services provided by the OCIO to the RNC are governed through a Service Level Agreement (SLA).

The purpose of the SLA is as follows:

> *OCIO provides Information Technology and Information management services to the Royal Newfoundland Constabulary. The services provided are governed through this service level agreement which is a collaborative agreement between the Office of the Chief Information Officer and the RNC.*
>
> *This agreement defines the scope, level and quality of Information Technology and Information management services the OCIO provides to the RNC. This agreement describes roles and responsibilities, mechanisms for communication, the dispute resolution process, and the process for adding new services.*

The SLA with OCIO establishes that it is the responsibility of OCIO to "incorporate information protection, IT security best practices as it relates to the RNC information." The SLA also has a confidentiality section that requires both parties to maintain the confidentiality of the information which is provided and received as part of the agreement.

The RNC is responsible for RNC records stored on equipment, with internet and intranet sites, in databases or any other devices provided by OCIO. This encompasses the lifecycle of the records, from creation to disposal. While not a comprehensive list, the RNC must also:

- Communicate IT/IM changes to the RNC staff;
- Provide security awareness information to IT/IM workforce provided by the OCIO, prior to the beginning of their work assignment;
- Request user access for the delivery of the services prescribed in this agreement. This shall include the addition of new user access, the deletion of users no longer needing access and the change access of current users;
- Request changes to the Charts of Authority and Charts of Responsibilities for applications that are unique to the RNC, where there are personnel changes in the RNC pertaining to the roles and responsibilities of these applications;
- Promote adherence to IT/IM Policies to all RNC staff which can be accessed at https://www.gov.nl.ca/exec/ocio/.

The SLA requires that all OCIO staff or contractors engaged by the OCIO that work on-site at the RNC have security clearance through the RNC security clearance process.

The SLA also ranks systems based on business composite impact, which is a combination of business needs, operational and public impact. The ranking is between 1 and 5, with those systems ranked at a 5 considered to have the most critical impact; the ICAN system is ranked at 5. It should be noted that this does not rank the sensitivity of the information contained in the system, merely the importance of the system to the day-to-day functioning of the public body.

The OCIO provides RNC employees with an email account, including storage space, backup and recovery services, wireless personal devices and web access. Authorized employees also receive a cell phone. The OCIO manages accounts based on information provided by the RNC, including account activation, user profiles, account suspension and account deletion.

RNC staff also have remote access and the OCIO provides the required equipment, software and internal access to remotely connect to the government's network.

In examining access controls, OIPC noted many strengths in the RNC system, including:

- Restricting remote access to systems, with the exception of systems designed to provide remote access. While remote access can be done securely, RNC has decided not to go this route for its systems at present.
- The systems designed to provide remote access feature additional safeguards, such as automatic locks in specific situations and not retaining information on the local drive.
- Requiring a separate login for certain systems and separate accounts for some as well. For some systems, if staff log out of their asset, they will need to log back into the system separately.
- Restricting user privileges for each system.

- Super users and administrators use two-factor authentication to access the systems and work is underway to expand this to encompass all users to two-factor authentication.
- Searches for some systems require specific details to be input, even when using the browse feature.
- The ability to use private or invisible features, which means that an entire record can be restricted or specific information within a record can be restricted. In the case of an invisible record, a query will result in no responsive records.
- Agreements are in place for external access to systems. The agreements discuss access level, set out the terms and conditions under which access to the system is granted, establish how the access can be used, how access will occur, and the process for obtaining access. It establishes who is responsible to provide system training and requires both parties to report any unauthorized uses or disclosures to the other. The agreement requires an annual meeting between the parties to review and assess the operation and effectiveness of the MOU. External users are also subject to the RNC audit program.

AUDITING

Even with access safeguards in place, auditing that tracks system access and use is a critical technological safeguard. It is best practice to have an auditing program, preferably with technical means to flag potential inappropriate access that is complemented by manual review.

Auditing is intended to monitor access to ensure it is appropriate and authorized. The Office of the Information and Privacy Commissioner of Saskatchewan and eHealth Saskatchewan developed guidance titled Auditing and Monitoring Guidelines for Trustees to assist in deterring, detecting and preventing unauthorized access to personal health information. It identifies three types of auditing and monitoring. First is proactive, where random audits are conducted on users. In healthcare, audits may also be based on clients, especially those identified as higher risk of privacy breaches, such as celebrities. The second is focused, where

an audit is conducted after a complaint is received. The final type is monitoring, which are less structured than the formal audits and can involve business rules that trigger alerts when abnormal or potentially inappropriate access occurs. In determining if the frequency of auditing represents a reasonable safeguard under *ATIPPA, 2015*, OIPC would consider the size of the organization, the number of users, the frequency of access to personal information, the sensitivity of the information, access by third parties and breach history. Any individual with access who has been found to have inappropriately accessed the system should be subject to more frequent random audits.

Order 339, issued on October 27, 2015, establishes that random audits of employees will be conducted. When issues are identified, follow-up is prompt and taken seriously. Routine Order 2016-018: Auditing of Motor Registration Division (MRD) and Integrated Constabulary Automated Network (ICAN) Systems came into effect on September 19, 2016, in part stemming from Report P-2015-002 involving three separate occurrences of privacy breaches at the RNC related to the inappropriate use of ICAN and MRD records. The Report recommended the implementation of a formalized auditing system for data accessible from both MRD and ICAN, as well as the development of related policies and procedures.

During the course of this audit, and in response to a recommendation from the OIPC Audit titled Information Sharing Agreements: Essential Administrative Safeguards, the RNC introduced Routine Order 2018-012, on the subject of MRD Searches and Potential Privacy Breaches. This Routine Order informed staff of the ISA in place regarding RNC access to the MRD database and requires all members (civilian and sworn) to review the ISA, with special attention called to sections 2.0 (Authority to Collect, Indirectly Collect, and Disclose Personal Information), and 4.0 (Confidentiality, Use, and Disclosure). The Routine Order directly addressed an issue raised in that audit, which involved a member searching their own name and license plate or those of family members for training purposes. It states: "This action is a breach of the Protection of Privacy Act and members are instructed to cease such activity."

The two public bodies worked together to identify a workable and realistic solution, with MRD creating training data for use during system training. The Order includes a list of queries that can be used, including names, drivers' license numbers and query plates. The Routine Order

does not establish the consequences for breaches of the MRD system, which is unfortunate given the breach history.

The RNC have a dedicated position to oversee the audit program and all staff with access to these systems are subject to at least one audit each calendar year. On a random basis, the audit manager selects samples from an employee's search history and verifies that the employee's search and corresponding file access was for a legitimate RNC business purpose. If supporting documentation cannot be found, the audit manager provides a standardized audit form to the employee's direct supervisor, who follows-up with the employee. Details are added to the form based on this follow-up and the form is then signed, with a copy retained by the supervisor and a copy returned to the audit manager. Even if no issues are found, the employee is notified that the audit occurred and reminded of pertinent policies. A sample e-mail provided by the RNC stated, in part:

> *Pursuant to RO-2016-18 (attached for your reference), your ICAN access is subject to random audit. I want to advise you that a sample of your ICAN search history has been reviewed and no breaches of privacy have been identified. No action is required on your behalf.*
>
> *For further information regarding privacy concerns and related audits, please refer to Section 7.0 of RNC policy entitled "Confidentiality" and Section 4.3 of RNC policy entitled "Information Management and Technology".*

Employees who are found to have inappropriately accessed information may face disciplinary action, have documentation of this placed on their record and be subject to additional auditing on a go-forward basis.

There is both a system log view, which could be considered a sneak peak, and a master log, which is a more detailed and robust audit log. The audit captures a number of actions, such as printing, which includes printing to PDF.

The audit program is more robust than just documenting the information accessed and following-up; it also involves critical thinking and analysis. For example, it is safe to assume that if a user in a police unit has accessed information over the MWS, that the other authorized

user in the vehicle is also aware of the data. Further, when concerns arise, it is possible to go deeper into systems and see what, if anything, has been changed.

The RNC have made improvements in auditing capabilities over the years. A requirement of the 2011 upgrade of the servers for CAD and RMS involved audit capabilities:

> *The application must maintain an audit trail which captures at a minimum:*
>
> - *Additions/Modifications to user access rights/permissions;*
> - *Amy and all action taken on an electronic records or its metadata*
> - *The identity of the user carrying out the action*
> - *The data and time of the action*
> - *The audit trail may not be altered*
> - *The audit trail of a record must be retained as long as the record to which it pertains*

PRIVACY IMPACT ASSESSMENTS (PIAS)

A Privacy Impact Assessment (PIA) is a recognized tool that assists in evaluating new and changed initiatives for privacy impacts, risk mitigation and legislative compliance. Often, a public body completes a Preliminary PIA (PPIA) to determine if a full PIA report should be completed. Such decisions are based on a number of factors, including the sensitivity and volume of personal information involved and the risks identified during the PPIA process.

The ATIPP Office's Protection of Privacy Policy and Procedures manual states:

> *A Privacy Impact Assessment (PIA) is an internationally recognized assessment method that can be applied to proposed programs or policies to identify potential privacy issues. PIAs examine such things as whether a proposed policy or program collects more personal information than is required, as well as the sharing of personal information that is collected; the access, storage, correction and disposal of personal information; and the proposed duration of the program or policy.*

A preliminary PIA (PPIA) was conducted on the ICAN system in 2011 and on the CCTV system in 2010.

OIPC would like to comment on the MOBL web application; while the focus of this audit is on current systems, the documentation prepared for the MOBL initiative should be recognized. MOBL was initially developed by the Government of Newfoundland and Labrador's Office of the Chief Information Officer (OCIO) in 2006 for Blackberry devices, however it is now deployed on RNC Mobile Workstations (MWS) located in patrol cars in the majority of cases.

When the MOBL project was first initiated, an MOU between OCIO and the Department of Government Services was signed, identifying the specific data fields that the RNC wanted to download from the MRD database to allow access to the Blackberries/Mobile Data Terminals. Please note that the data would not be downloaded to the mobile devices, rather access to a copy of the data would be facilitated. The MOU also identified the purpose for the access and made a commitment that the Department of Justice would ensure that it was not used for other purpose.

The document "A Co-Operative Proposal: MRD Police Information Extract" provided much detail about the project and in fact, contains most of the background information this Office would expect from a PIA. Under the process at the time, an RNC officer on patrol would be required to contact the switchboard over the radio to obtain information about a licence or a vehicle. In addition to requiring resources from the switchboard operator, the radio system and the officer, it also exposed the individual's personal information to a second user (the switchboard operator) and anyone within hearing of the radio. The updated system allows an officer to locate the required information using a Blackberry device that automatically locks when placed back on the officer's belt clip or the inactivity timeout was reached. The solution represented an improvement to flow of work and privacy protections.

While the proposal did not really discuss privacy risks in great detail, it represents solid documentation of the current and the future state, with details of how this represents an improvement over existing process. This is critical information for any privacy assessment, as it provides the details necessary to recognize that, while privacy risks still exist, the new system actually represents an overall improvement in privacy protections. Further, the OIPC has long expressed that the format and name of the assessment is not as important as the content of the assessment itself.

POLICIES AND PROCEDURES

A common administrative safeguard is policies and procedures. In 2011, the Privacy Commissioner of Canada released an Audit of Selected RCMP Operational Databases. The audit examined the policies and procedures in place to ensure the appropriate level of access, given the sensitive nature of the personal information at issue. In addition, it looked for compliance checks to ensure inappropriate disclosures were not occurring.

This Office expects to find detailed policies and procedures in place regarding system access and training requirements, as well as evidence that compliance checks had been completed. Developing policies and procedures is merely the tip of the iceberg; organizations must also train staff, ensure that staff understand how the policies and procedures apply in their roles, as well as check to ensure staff are complying with them. Further, it is important that policies and procedures detail the consequences of non-compliance and that staff are aware of those consequences.

The RNC maintains an intranet-based policy and procedure manual for its officers and civilian staff detailing approximately 150 policies and procedures guiding the RNC's operations. Topics addressed include: the RNC's organization and structure, its guidelines for responding to particular criminal offences, conducting investigations, recruitment, uniform standards and many others. The Chief of the RNC also, from time to time, issues Routine Orders amending the RNC's policies and procedures. The policies and procedures are considered instructions and guidelines for police officers and civilian staff. When new members are sworn in, they are given a copy of all policies.

RNC directives and agreements clearly establish acceptable uses, the individuals responsible for ensuring compliance with the directive and the consequences of non-compliance. Further, the RNC has a number of policies in place that detail many points of interest for this audit. Staff who read the policies should have a good grasp of why they have access to RNC information assets, as well as what they are allowed to do with it.

The *RNC Information Management and Technology Policy and Procedure Manual* contains policies and procedures, as well as general orders. While the entire manual was not reviewed as part of this audit, following is a discussion of manual content most applicable to this audit.

General Order 339, issued on October 27, 2015, addresses confidentiality. It states, in part:

> *The RNC has both a legal and ethical responsibility for the information generated within the fulfillment of its mandate as a police service, and, the RNC is committed to protecting the privacy of personal information and the confidentiality of the law enforcement information in its custody and control.*
>
> *It is the responsibility and obligation of RNC employees, to ensure that information to which they have access is kept private and confidential.*

This Order reflects requirements established in the *Royal Newfoundland Constabulary Act*. Section 60 recognizes the importance of confidentiality, stating in part:

> *60.(1) A police officer, an employee of the constabulary, an investigator, the commissioner, adjudicators and all persons acting under this Act shall preserve secrecy in respect of all information obtained in the course of their duties and shall not communicate that information to another person except* ***...***

The Order clarifies the information that should be treated as confidential, stating in section 3.4, that, "Information that is to be kept confidential and private is information that would not otherwise be publicly available." Section 3.6 lists various categories of confidential information and private information with examples of each, including categories for personal information, operational/service delivery, administrative, financial, human resources, legal, business and other initiatives, and other. This audit is only examining personal information.

The Order further requires information obtained in the course of employment to be held in confidence and that reasonable measures be taken to ensure that collection, use and disclosure of information is necessary and authorized before collection, use or disclosure occurs. This should assist in ensuring that the minimum amount of personal information necessary for the identified purpose is collected and added to the systems subject to this audit, and that the minimum amount of personal information necessary is subsequently used and/or disclosed.

The Order also addresses accountability for breaches of confidentiality and/or privacy. It defines a breach as:

> *…intentional or unintentional unauthorized access to, use and/or disclosure in any manner (including written, electronic or verbal), directly or indirectly, of confidential or private information. A breach includes unauthorized access to recorded and/or unrecorded information including written, electronic and/or verbal information.*

It requires all employees to immediately report a breach or suspected breach and establishes that those individuals deemed responsible may face penalties and discipline. It also notes that random audits of employees will be conducted.

This is consistent with section 3(1) of the Royal Newfoundland Constabulary Public Complaints Regulations, which states in part:

> *3.(1) A police officer shall not conduct himself or herself in a manner unbecoming to a police officer and liable to bring discredit upon the Royal Newfoundland Constabulary, which shall include but not be limited to the following:*
>
> *…*
>
> *(f) without proper authority, disclose, directly or indirectly to a person, information which he or she has acquired as a police officer;*
>
> *(g) attempt to commit, aid, abet, counsel or procure another police officer to contravene these regulations;*
>
> *…*
>
> *(j) carry out his or her duties in a manner contrary to the Policy and Procedures Manual;*
>
> *….*

While the above only applies to police officers, the Order applies to both officers and civilian staff. Having an Order apply to all staff ensures consistency and reflects best practice.

Staff acknowledge the requirement for confidentiality and applicable policies and procedures through an Oath/Affirmation of Confidentiality. The Order establishes that all RNC employees, and persons who participate in an RNC ride-a-long, complete an oath or affirmation of secrecy at the commencement of employment, association, affiliation or training with the RNC. This

is also required by section 5 of the *Royal Newfoundland Constabulary Act*, which states, in part:

> *5.(1) Before commencing his or her duties of office every police officer and every other person employed in the constabulary shall swear or affirm an oath or affirmation of office and secrecy as prescribed by regulation….*

The importance of the Oath is reaffirmed in Routine Order 2013-002, titled Oath of Confidentiality and Social Networking. This reminds staff that they have sworn an Oath to "….not, directly or indirectly, without due authority, disclose to any person any information or other matter that may come to me in the performance of my duties as an employee…" This Order also establishes that employees must not use social networking sites, such as Facebook, to engage in communication regarding workplace topics. It further states, "Any social media posts in relation to your employment may be considered a breach of confidentiality and a potential security breach."

Such reminders throughout an individual's engagement with an entity are critical safeguards.

In addition to orders on training and confidentiality, General Order 322 (Information Management and Technology) addresses a number of topics, including security, employee expectation of privacy, e-mails, appropriate use of information resources, and personal information protection, as well as outlining roles and responsibilities. For example, section 4.5 has a list of user requirements that address issues such as passwords.

While the following is not a comprehensive summary of the policy, the sections most applicable to this audit include:

> *1.3 The Information Services Division is responsible for planning, developing, organizing, directing and managing the Information Management and Technology program in partnership with the Office of Chief Information Officer (OCIO).*
>
> *…*
>
> *3.5(a)(1) Computer equipment and resources are provided to employees to conduct government business.*
>
> *…*
>
> *4.3. Access by employees to RNC information for personal reasons or non-law enforcement related reasons is prohibited and any improper access by an*

employee will cause an employee to be subject to discipline up to and including dismissal.

…

4.6 The following conditions are unacceptable and will result in discipline up to and including dismissal.

a. Users must not:

…

(3) use the Employer's equipment for personal purposes;

…

(5) install any hardware including but not limited to; personal USB drives, personal cell phones, personal external hard drives or any peripherals, or software (computer games, screen savers or utilities and any software downloaded from the internet or from another medium) on computers operational within the RNC unless specifically authorized by the OCIO;

…

(8) utilize someone else's user identification or password to gain access to a network resource without proper approval;

…

(15) access the RNC network using their own personal equipment (e.g. personal Laptop, IPad, etc.); and

…

7.4 Managers/Supervisors are responsible for:

a. ensuring requests for network and database access are forwarded to the OCIO Service Desk following transfers to any new Division;

b. ensuring that authorized individuals in the Division use their access to departmental systems for government business and other authorized purposes only;

c. ensuring that divisional employees adhere to all network and computer resource usage related policies;

…

Some of the responsibilities identified in the policy reinforce requirements established in the Royal Newfoundland Constabulary Regulations. Section 6(2) states:

6.(2) A supervisor shall ensure that police officers coming under his or her supervision will adhere to all directives, memorandums, policies and procedures as approved by the Chief of Police and is responsible for reporting to his or her immediate supervisor any police officer who fails to carry out his or her duties in a manner as required by the directives, memorandums, policies and procedures not considered of a minor nature.

> ...

Routine Order 2015-002, titled Appropriate Use of RNC Records and Information, emphasizes what constitutes an appropriate use to staff, stating, in part:

> *All staff are reminded that RNC records and information is strictly for **official duties related to law enforcement**. Access to RNC information for personal reasons or non-law enforcement related reasons is strictly prohibited.*
>
> ...
>
> *Individuals will be held accountable for breaches of confidentiality or privacy regarding RNC records or information. A breach includes unauthorized access to, use or disclosure in any manner (including written, electronic or verbal) of RNC records or information.*

TRAINING

Training is an important safeguard that assists public bodies in complying with section 64 of *ATIPPA, 2015*. All public bodies should have an education program that consists of training and awareness activities. Training may be general, such as an introduction to applicable legislation, like *ATIPPA, 2015* and the *Royal Newfoundland Constabulary Act*, as well as system specific training that introduces end users to the system, outlines acceptable uses and calls attention to applicable policies and procedures. Organizations should employ both for employees whose job involves access to personal information. Awareness activities should reinforce key messages and remind staff of obligations, especially when gaps are identified. While general training is valuable, it is important to provide complementary training to assist staff in connecting broad concepts to their specific roles and daily tasks. Further, training should be ongoing to keep current on the changing operating environment, when new employees are onboarded, and other junctures where gaps in knowledge are reasonably foreseeable.

OIPC Report P-2018-002 states that, "A system of safeguards that omits regular and continuing privacy training fails to meet the standards set out in section 64 of the *Act*." In Report P-2018-001, we also commented on training, stating "If its employees receive no or inadequate training with respect to the legal requirements of *ATIPPA, 2015*, and in particular as to what constitutes unauthorized collection, access, use or disclosure, a public body has

not met its obligations under section 64." In paragraph 18 of that Report, two recommendations focused on training, with one requiring staff with access to personal information to receive formal privacy training and the second to develop policies addressing privacy training for new hires, and annual training for all staff with access to personal information.

In Securing personal information: A self-assessment tool for public bodies and organizations, nine training criteria are listed under the Human Resources Security section of the checklist:

> *Has training been implemented for all employees, data custodians and management to ensure they are aware of and understand:*
>
> *4.4 Their security responsibilities?*
> *4.5 Security policies and practices?*
> *4.6 Permitted access, use and disclosure of personal information?*
> *4.7 Retention and disposal policies?*
> *4.8 Requirements for password maintenance and proper password security?*
> *4.9 Is annual privacy and security training a requirement for any handling of personal information?*
> *4.10 Are there consequences, such as blocking access to personal information, if employees do not complete annual privacy and security training?*
> *4.11 Are there consequences for compromising keys, passwords and other security policy violations?*
> *4.12 Is completion of privacy and security training tracked?*

The checklist also addresses Confidentiality Oaths/Affirmations. It asks if the oaths/affirmations clearly define individual responsibilities for protecting personal information, and if individual performance related to security and confidentiality are regularly reviewed, among other criteria.

Another publicly available resource that discusses policies and procedures related to training is a 2015 presentation from OIPC Ontario called Protecting Health Information In an Electronic Environment. Considerations included the requirement to provide and attend initial and ongoing training; the identification of an individual responsible for developing and implementing training; establishment of the minimum content for training materials; requirement to review and refresh materials, including the identification of the individual responsible and the frequency of the review; requirement to track attendance at training

sessions; the consequences for failure to attend sessions; and identification of other mechanisms to promote a culture of privacy.

The RNC issued Routine Order 2016-16 on September 1, 2016; *Subject: Mandatory Training. Access to Information and Protection of Privacy*. It requires all employees to complete the online Access to Information and Protection of Privacy e-learning course offered through the Centre for Learning and Development, Human Resource Secretariat. The order stated, "This training outlines the obligations of the RNC and all employees' responsibility in the access to information and protection of personal information." While the Order required all staff (sworn and civilian) to complete the training by a specific date and the training was tracked by the Training Section, the Order did not identify any consequences of non-compliance.

This training is described on the HRS site as:

> *This module is intended to give participants an understanding of their responsibilities as public body employees to uphold access and privacy provisions. This is done by providing an introduction to access and privacy principles and Newfoundland and Labrador's Access to Information and Protection of Privacy Act (ATIPPA).*

This Office has examined this training module in previous reports, including Report P-2018-002, which stated, "This 45-minute exercise should be a part of onboarding and required for completion on the first day of employment for all public body employees." That Report established further training expectations, noting:

> *[20] Further, the online ATIPP training requires supplementation in the form of attending a session delivered by subject matter experts. The provincial ATIPP Office and the OIPC both offer to provide training at no cost to public bodies. Continuing education is also necessary to refresh the importance of privacy and update employees on current developments. It is the responsibility of managers, and ultimately the head of the public body, to ensure that the level of training provided is appropriate to the degree of sensitivity of information handled and the degree of access to that information provided to employees.*

During the course of this audit, the RNC invited OIPC staff to conduct training sessions, which were completed. The OIPC receives requests for staff training from public bodies and we accommodate those whenever possible.

When it comes to system specific training, the RNC submitted the training manual for the ICAN system to the OIPC for review. Training on the ICAN system is quite detailed, with five modules that take approximately 21 hours to complete. The ICAN Training is developed and delivered by the RNC Information Services Division (ISD); it includes generic information provided by the vendor and local information developed by ISD. In additional to manuals with exercises, there are slide decks for some modules to add emphasis to key points.

The training objectives for the ICAN system are clearly defined and includes quizzes at the end of each day and a test at the end of the week. Test results are retained in the training database. This training applies to all staff; cadets and new hires attend more detailed training, while communication technicians only attend the CAD training. Once the formal training is completed, all staff receive side-by-side training on all systems, where a trainer/more experienced user provides hands-on instruction, and the new user is able to start to apply their knowledge and use the systems for work purposes.

While there are over 400 pages of step-by-step instructions on using the system, the training is light on acceptable system use; RNC informed OIPC that it does include discussion of the probationary period. The slide deck that accompanies the "Query and Browse" section (module 4 part 5) does have a "Policies" slide that states,

> *Information accessible to members is only for official duties related to law enforcement and related operating programs and activities (RNC IM/IT Policy). All requests for statistical reports for both external agencies and internally is the responsibility of Information Services Division (RO 2005-002).*

The training slide for the MOBL system states, among other things:

- RNC use only;
- 100% comprehensive auditing; available to MRD;
- User account access auditable by MRD.

Staff should know why they have access to ICAN, acceptable uses of the systems and uses that would be considered inappropriate and possibly breaches. That said, the training emphasizes many important privacy principles, including the importance of complete and

accurate information, as well as the terms to use for various situations that would ensure consistency in documentation.

It is important to note that all RNC systems have both a production and a development/training environment. This ensures that individuals learning to use systems are not exposed to live data, yet are still able to get hands on experience on how to use the systems.

As well, every Wednesday training is offered to Officers; this ongoing training is an opportunity to ensure Officers are aware of expectations and to address any topics of interest or issues. The RNC has dedicated training section that manages all aspects of training.

While directives clearly define acceptable system use, as well as general acceptable uses of all personal information to which staff have access, there is no indication that these directives are addressed in the system-specific training provided to staff. Staff who are trained on system usage should be trained on why they have access and what they are allowed to do with that access at the same time. Further, the RNC provided no documentation to establish that regular privacy training occurs, either general or system specific.

That being said, although this Office did not attend a training session, it did review the *ATIPP for RNC Employees* training slide deck provided by the RNC. This is one of two training sessions that are delivered to all new members; the second is called Information Management and Technology Guidelines. For the most part, the slide deck addresses disclosure and access to information, with a reminder about the Oath of Secrecy. The protection of privacy slide states:

> *Part 2 Protection of Privacy*
>
> *Three points*
>
> - *When is it okay to for a police officer to access police information*
> - *When is it okay for a police officer to disclose police information*
> - *What can you say on facebook*

The following slides provide examples and additional information on this slide. For example, another slide asked, "Can you Look for the Wrong Reason without getting in Trouble?" The response is "No". However, the slide deck does not expand on the term "trouble." In addition to internal discipline according to human resource policies, section 115 of *ATIPPA, 2015* establishes that an individual who willfully collects, uses or discloses personal information in contravention of the *Act* is guilty of an offense. If convicted, the individual faces a fine of up to $10,000 and/or imprisonment for a term not exceeding six months. RNC employees have been prosecuted under this provision in the past, so it is important that some awareness that this is a potential consequence be incorporated into training.

The RNC's training slide deck also reinforces messaging in policies and routine orders; for example, one slide deck notes that staff are not allowed to use personal devices with work assets.

The slide deck called Information Management and Technology Guidelines was also reviewed by this Office. While OCIO provides information technology and information management services to the RNC, a slide on this deck indicates that:

> *IT staff are forbidden from reading network data, e-mails or database content except under the following conditions:*
>
> - *Conducting support for the data owner*
> - *Responding to a written request from the employees supervisor or Divisional Commander*
> - *Responding to a written request from the IT Security Committee*

The slide deck highlights that security is the responsibility of all employees that have access to, use or manage the information and technology assets of the RNC. It also emphasizes that equipment and access are provided for the purpose of conducting business and employees should have no expectation of privacy. There is a slide that details Appropriate Use of Information Resources that states, in part:

> *Access by employees to RNC information for personal use or non-law enforcement is prohibited and any improper access by an employee will cause an employee to be subject to discipline up to and including dismissal.*

In a slide on security breaches, an example of unacceptable activities that will result in discipline includes installing any hardware on computers operational within RNC, including personal USB drives and personal cellphones. Staff are not allowed to access personal e-mail accounts or chat utilities from within the RNC network. Staff cannot access the network using a personal device, such as a laptop, and the training specifically forbids staff to: "Configure a government e-mail account to automatically forward incoming messages to a non-governmental email account."

In addition to training, awareness activities are good options to ensure staff are reminded of key training content and to address issues as they arise. The RNC conducts random audits as per General Order 339 and uses this as an opportunity for acceptable use awareness. When an audit is conducted, the individuals subject to the audit are notified by letter, even if the audit is clear. The RNC indicated that this keeps staff aware that someone is watching their actions and reminds them that there is an audit trail. This is a great way to turn an existing activity into an awareness activity. The RNC have also made system training videos available on the RNC shared drive to allow individuals to access training on an as-needed basis. For example, if a particular module has not been used much since training, the individual may wish to re-fresh on that particular aspect of the system.

OBSERVATIONS AND RECOMMENDATIONS

ACCESS

ATIPPA, 2015 requires that public bodies collect the minimum necessary information for the identified purpose and to ensure reasonable safeguards are in place to protect that personal information. Further, public bodies may only collect, use and disclose personal information in compliance with the legislation; that is, they need authority to collect, use or disclose. It is difficult, if not impossible, to comply with the legislation if a public body cannot identify what personal information it has, where it is located, who has access, and how it is protected.

While the RNC were able to provide high-level descriptions of the information it has in the systems subject to this audit, it lacked specific details on the information. For example, no complete list of data fields was provided. While some detailed descriptions and

categorizations of the information was located in different documents, such as Pre-Threat Risk Assessments and Information Security Classifications, there was no main inventory provided to OIPC. It is difficult to determine appropriate access if a clear and robust description of the information contained in the systems is not readily available.

Recommendation #1

The RNC develop a personal information inventory that meets the requirements established in OIPC's Privacy Management Program guidance. Specifically:

An inventory should include a description of the following:

- the types of personal information and/or personal health information the organization holds (ex: names, home addresses and contact information of clients);
- the sensitivity of the information;
- where the personal information and/or personal health information is held, both within the organization (ex: paper files in staff offices and electronic information in a database) and where it is held by third parties (including service providers);
- the purposes for which the information is collected, used and disclosed and how each piece of information collected contributes to the purposes; and
- the details of the retention schedule and any requirements for secure destruction.

Public Body Response

The Royal Newfoundland Constabulary agrees with this recommendation.

Throughout the audit, it was obvious that the RNC has staff that are knowledgeable about the systems and associated safeguards. However, gaps in documentation exist. When conducting an audit using the Generally Accepted Privacy Principles (GAPP) criteria, there are a number of maturity levels, ranging from ad hoc to optimized. Not all of the GAPP criteria need to be at the optimized level, however entities need to be aware of gaps and assess the risk these gaps represent.

Recommendation #2

> RNC conduct its own audit of systems documentation, identify risks and assess if there are gaps that need to be addressed.

Public Body Response:

The Royal Newfoundland Constabulary agrees with this recommendation.

The RNC has agreements in place with the RCMP's Canadian Firearms Program (signed in 2015) and the RCMP's B Division (signed in 2002). The latter agreement doesn't contain some of the safeguards mentioned in the former agreement, including review and the requirement to report unauthorized uses and disclosures.

Recommendation #3

> RNC update the agreement, leveraging the improvements made in the most recent agreement during this update.

Public Body Response:

The Royal Newfoundland Constabulary agrees with this recommendation.

IT SUPPORT

The OCIO has established standards for all government assets; RNC assets are subject to these standards. It should be noted that OCIO standards represent the minimum level of acceptable safeguards and entities should satisfy themselves that the level is appropriate for the specific information and systems involved; they are able to establish more stringent safeguards if assessed as appropriate.

Further, entities that rely on OCIO Standards should know details of the standards. During the course of this audit, when asked for details of certain safeguards, RNC indicated that they complied with OCIO standards, without consistently providing details of those standards.

Recommendation #4

> RNC ensure that all OCIO standards that are followed are documented, along with an assessment to determine if those standards are reasonable for the system and information contained within.

Public Body Response:

The Royal Newfoundland Constabulary agrees with this recommendation.

The RNC, like many other public bodies in the province, relies on OCIO for IT and other services. The services provided by the OCIO to the RNC are governed through a Service Level Agreement (SLA) that was signed in 2008.

Recommendation #5

> RNC review this agreement and sign once updated to the satisfaction of both parties.

Public Body Response:

The Royal Newfoundland Constabulary agrees with this recommendation.

AUDIT

The audit trail for RNC systems varies, with some actions not captured and some systems only audited upon request or when potentially inappropriate actions in other systems are flagged. The RNC indicates that the risk of audit shortcomings is mitigated by the sensitivity of the information contained within these systems.

Auditing is a labour intensive job that requires multiple individuals. When the auditor locates a potential anomaly, they first need to follow up with the manager and then the individual. Having an automated tool that identifies potentially abnormal activities would focus the auditor's efforts. For example, an automated tool could flag potentially abnormal accesses based on criteria such as accessing information outside of normal working hours, logging in at two separate locations at the same time, registering a high number of errors or searching same last name or same address.

The random audits currently being conducted do mitigate some of the risks presented by not having a more robust audit program. However, no documentation was provided on how the RNC selected annual audits; how was this frequency identified and determined to be reasonable?

It should be pointed out that the snooping that has occurred may not have been revealed through a more robust audit program. The snooping incidents involved people known to the individuals involved; this type of issue is difficult to proactively predict and has as much to do with the screening of candidates, organizational privacy culture, and staff training as it does anything else.

Recommendation #6

In general, the RNC's controls to detect and prevent inappropriate employee access and use of personal information are limited by the lack of an automated tool to identify and flag potentially inappropriate accesses. OIPC recommends

that RNC investigate automated auditing to determine if there is a product that would address current gaps.

Public Body Response:

The Royal Newfoundland Constabulary agrees with this recommendation. Since the commencement of this audit in 2017 the Audit and Compliance Manager for the RNC has established some audit triggers as a part of their process to detect some abnormal activities by users. The Royal Newfoundland Constabulary agrees to further investigate the potential for automated auditing compatible with our systems.

PRIVACY IMPACT ASSESSMENTS (PIAS)

While a PPIA was conducted on the ICAN system in 2011, it lacks the detail necessary to understand the system, the information contained within and the risks associated with the system. A PIA should examine the system in its entirety, including how users can access the system and what different access roles are available. The information contained in a privacy assessment for a system with a high volume of personal information of a large number of individuals should be quite detailed, For example, all RNC systems have limits on the number of times an incorrect password can be entered before an account is locked, however specific details of passwords were not documented. The complexity requirements, length, frequency of changes, how often the password can be repeated, etc. are important to know when assessing the reasonableness of safeguards.

Further, Report P-2015-002 recommended that the RNC complete a PIA of the ICAN database; although this Office has met with the RNC to discuss this recommendation, a PIA has yet to be completed. A PIA is an important tool that can help ensure and demonstrate compliance with Part III (Protection of Personal Information) of *ATIPPA, 2015*.

During the audit, OIPC inquired about updated privacy assessment documents or if a full PIA had been completed on the ICAN system. The RNC indicated that, because ICAN existed on an isolated network with no remote user access to the system and was subject to a NCACR

(Net Connection Authorization Change Request) submission every two years to ensure compliance with RCMP IT requirements, a full PIA was not necessary.

The OIPC did not see any documentation of these details in the Privacy Impact Report provided to this Office, it merely concluded that a full PIA was not necessary at that time. Further, while these safeguards may lower the risk faced by the system, risks still exist. Finally, PIAs are living documents that should have a review schedule. Even with a review schedule, changes may occur that prompt a review. Since the original PPIA was conducted, changes occurred to the system and to *ATIPPA, 2015*. Both these factors would generally trigger a review.

While a PIA was conducted on the CCTV system in 2010, no documentation was provided to demonstrate that follow-up had occurred on the four recommendations contained in the Report. Over the years, PIA templates and processes have changed, as privacy protection has matured.

OIPC would again like to comment on the documentation available for the MOBL web application; the MOU and initiative proposal are documents that could be leveraged for the PIA. Many initiatives have supporting documentation that could be attached to a PIA or used for PIA content.

It needs to be noted that the lack of PIA and other documentation does not mean that safeguards are not in place. What it means is that there is insufficient documentation of a detailed and robust review having been conducted on the ICAN system. Given the volume of personal information contained in the system and the number of individuals with access, this is an important step to document consideration of and compliance with the requirements of *ATIPPA, 2015*.

Recommendation #7

RNC conduct a comprehensive privacy assessment on the ICAN system; this assessment should comply with the review expectations established in OIPC's PPIA/PIA Review Criteria. This guidance outlines critical content for privacy

assessments, as well as considerations for when a full PIA is recommended. Given the volume of information contained within the ICAN system, the fact that at least some would be considered sensitive by individuals, the high number of individuals with access, documented snooping incidents, the fact that some information may be collected indirectly either from other individuals or systems, and the increasing number of cyber attacks occurring internationally, OIPC has concluded that a full PIA is required.

Public Body Response:

The Royal Newfoundland Constabulary is in the process of hiring a dedicated resource for the purpose of administering the *Access to Information and Protection of Privacy Act, 2015*. Once that position is in place the RNC will again review this recommendation.

Recommendation #8

RNC attach an appendix to the CCTV Privacy Impact Report with an update on the recommendations made in 2010.

Public Body Response:

The Royal Newfoundland Constabulary agrees with this recommendation.

POLICIES AND PROCEDURES

It is obvious that the RNC have put great effort into developing comprehensive policies and procedures. Without written policies and procedures, an organization's compliance with *ATIPPA, 2015* will be ad hoc and potentially haphazard. Further, policies help employees to understand their privacy obligations and how to fulfill them. Please note that the scope of this audit did not include examination of any compliance work conducted by the RNC to ensure staff were aware of and complying with policies and procedures; the audit focused on the content of existing policies and procedures only.

Recommendation #9

RNC modify existing policies or create new policies that:

- clearly states that RNC is a public body subject to *ATIPPA, 2015;*
- establishes when a privacy assessment be conducted, including clear guidelines on when a PPIA will trigger a full PIA.

Public Body Response:

The Royal Newfoundland Constabulary agrees with this recommendation. Our Information Management and Technology policy, last updated in October 2021, does touch on the topic. The RNC will review and update accordingly.

Recommendation #10

Policies and Orders be reviewed to ensure they reflect at minimum the legislative definition of breach in section 64(4) of *ATIPPA, 2015*:

64(4) Where the head of a public body reasonably believes that there has been a breach involving the unauthorized collection, use or disclosure of personal information, the head shall inform the commissioner of the breach.

Public Body Response:

The Royal Newfoundland Constabulary agrees with this recommendation. Section 5 of our Confidentiality policy, last updated in May 2022, includes this recommendation. The RNC will review and update accordingly.

TRAINING

It is not enough to have policies and procedures in place; staff must be trained on the policies and procedures in order to understand both how they apply in their role and the consequences of non-compliance. In the context of access to personal information, it is important for staff to understand the acceptable use for all personal information to which they have access and the

consequences of inappropriate collections, uses and disclosures, which should include the possibility of penalties up to and including termination.

The expectations of OIPC for RNC training were clearly established in Report P-2015-002, which states in part:

> *[32] Consequently, while privacy training and oaths of confidentiality are conducted by the RNC, additional training is required. The training must cover the definition of "personal information", auditing, unauthorized access and disclosure, proper use of personal information, the "need to know" principle and privacy versus confidentiality.*

Two recommendations stemming from this Report addressed training, stating:

> *(c) all staff should complete privacy training each year that includes a comprehensive privacy tutorial with specific modules on privacy issues related to electronic information systems and the other topics I have outlined above. Completion of this training should be tracked in each employee's personnel file and linked to an annual renewal of user privileges;*
>
> *(d) oaths of confidentiality or oaths of office should also be revisited and amended as necessary when employees change roles. These undertakings should reflect the "need to know" principle;*

Outside of a requirement for the ATIPP Online training, there was nothing specific about training in the policies and procedures provided to our Office. Documenting training requirements in policy and procedures ensures consistency across the organization and demonstrates commitment to the topics listed in the policy. The RNC does have a Training Section, which provides a foundation to implement any training policy.

Training is an important safeguard that assists public bodies in complying with section 64 of *ATIPPA, 2015*. Lack of awareness of policies, procedures and legislative requirements cause breaches and issues with compliance. It is best practice to offer ongoing, mandatory education with the goal being that all employees will understand their role in information protection, why they have system access and any consequences of deviating from expectations. All public bodies should have an education program that consists of training and awareness activities.

Recommendation #11

RNC develop a training and awareness program. The program should focus on policies and procedures (new and reminders), systems (why users have access to individual system), privacy basics like the definition of "personal information", the RNC auditing program, implications of unauthorized access and disclosure, proper use of personal information, the "need to know" principle and privacy versus confidentiality.

The program should also establish the frequency of training; OIPC recommends at least every two years, however is open to hear RNC's need assessment on the frequency.

Public Body Response:

The Royal Newfoundland Constabulary now routinely distributes messaging regarding privacy through the use of email. Topics covered in the communications vary including but, not limited to examples of personal information, examples of appropriate and inappropriate queries of the RNC systems, information about privacy audits and, privacy tips and information specific to law enforcement. The Royal Newfoundland Constabulary is working to develop a more formal process for providing employees with timely information and reminders.

Additionally, the Royal Newfoundland Constabulary accepts the recommendation of every two years for the frequency of privacy training.

Recommendation #12

Expand the ICAN training to include why staff have access to ICAN, acceptable uses of the systems and uses that would be considered inappropriate and possibly breaches.

Public Body Response:

The Royal Newfoundland Constabulary agrees with this recommendation. The RNC has updated its ICAN training to include this information since the commencement of this audit.

CONCLUSION

I would like to take this opportunity to thank the staff and leadership of the Royal Newfoundland Constabulary, particularly Chief Patrick Roche and Kim Harding - Executive Director of Support Services, for their cooperation and assistance during this audit, and for the constructive and positive response to our recommendations. It is my hope that the RNC finds this audit useful in your continued efforts towards improvement and best practice.

Michael Harvey
Information and Privacy Commissioner
Newfoundland and Labrador