Audit of Emerging Investigative Technologies

Vetted Report

September 2023

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Aussi disponible en français sous le titre : Vérification des nouvelles technologies d'enquête

For more information, contact:
Internal Audit, Evaluation and Review
Royal Canadian Mounted Police
73 Leikin Drive
Ottawa, Ontario, Canada
K1A 0R2

www.rcmp.ca

Catalogue Number: PS64-228/2024E-PDF
ISBN: 978-0-660-71537-7

Access to Information Assessment

This report has been reviewed in consideration of the *Access to Information Act* and *Privacy Acts*.

[REDACTED] appears where sensitive information has been removed in accordance with the principles of the *Access to Information Act* and the *Privacy Act*. Published information is UNCLASSIFIED.

Table of Contents

ACRONYMS AND ABBREVIATIONS

List of Acronyms Used	
AI	Artificial intelligence
AIA	Algorithmic impact assessment
ASB	Air Services Branch
ATIP	Access to Information and Privacy
BWC	Body-worn camera
CE	Classified environment
C&IP	Contract and Indigenous Policing
CM&C	Corporate Management and Comptrollership
CODI	Committee on Digital Investments
CROPS	Criminal Operations Officer
DNA	Deoxyribonucleic acid
DS	Departmental Security
EDI	Equity, Diversity and Inclusion
EIT	Emerging investigative technology
FAA	Financial Administration Act
FPCO	Federal Policing Covert Operations
GBA Plus	Gender-based analysis plus
GC	Government of Canada
GG	Genetic Genealogy
IACP	International Association of Chiefs of Police
IGGT	Investigative Genetic Genealogy Technique
IM/IT	Information Management/Information Technology
IOPC	Investment Oversight and Prioritization Committee
LAST	Legal Application Support Team
MAP	Management Action Plan
MCM	Major Case Management
ML	Machine Learning
NCROPS	National Criminal Operations
NDDB	National DNA Data Bank
NOISP	National Office of Investigative Standards and Practices
NTOP	National Technology Onboarding Program
OPC	Office of the Privacy Commissioner of Canada
PIA	Privacy Impact Assessment
PSPC	Public Services and Procurement Canada
RCMP	Royal Canadian Mounted Police
RODs	Records of decisions
RPA	Remotely-piloted aircraft
RPAS	Remotely piloted aircraft system
SD	Secure digital
SEC	Senior Executive Committee
SME	Subject-matter expert
SOPs	Standard operating procedures
SPS	Specialized Policing Services
St. ROCH	RCMP Operational Centralized Holdings
SUA	Small Unmanned Aircraft

TB	Treasury Board of Canada
TBS	Treasury Board Secretariat
UHR	Unidentified Human Remains
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle

EXECUTIVE SUMMARY

BACKGROUND

The Royal Canadian Mounted Police (RCMP) 2020 Environmental Scan identified that the world is undergoing a fourth industrial revolution whereby innovation is driving the emergence of new technologies at unprecedented rates, and individuals are gaining expanded access to these advancements. Technology is becoming increasingly connected, merging the digital and physical realms in new ways that uniquely enable both law enforcement and criminality.

While these innovations have resulted in tech-savvy criminals driving the increase of technology-based crimes, emerging technologies also provide law enforcement with new methods and means to investigate and prevent crime, increase employee and public safety, and improve access to information for timely decision-making.

Emerging investigative technology (EIT) is a concept without a formal definition in Treasury Board (TB) policies or the RCMP. EIT used by law enforcement can encompass:

- Physical equipment, such as automatic licence plate readers, remotely-piloted aircraft systems (RPAS), and Body-worn cameras (BWC),
- Information management/information technology (IM/IT) tools or software such as media aggregation tools, artificial intelligence (AI) and machine learning (ML), decryption tools and on-device investigative tools,
- Forensic science-driven technologies such as genetic genealogy (GG), genetic profiling, biometrics (facial and voice recognition).

EIT can be a good purchased off the shelf, a technology developed in-house, or a service acquired through a third party.

Due to the speed at which these new investigative technologies emerge and the relative ease by which they can be publicly acquired and accessed, many are not yet governed by legislation or policies.

WHY THIS IS IMPORTANT

It is important for the RCMP to be properly equipped to combat the changing nature of crime by leveraging EIT when appropriate and within the legislative framework, and broadly speaking, in a manner that meets public scrutiny.

Creating a robust framework for technological innovation, and the lawful onboarding of new techniques to support criminal investigations can be inherently complex. It entails the retention, recruiting and training of personnel with the appropriate skills and competencies to use, support and maintain EIT. This creates challenges and opportunities, more than ever before on the RCMP's IT infrastructure and systems to support the organization in delivering core services and addressing future priorities.

This audit is intended to support the RCMP in achieving its modernization objectives related to operational tools, equipment and technologies, which is a priority identified in Vision 150 and Beyond: RCMP Strategic Plan. For these reasons, the RCMP Risk-Based Audit and Evaluation Plan 2021-2026 included the Audit of Emerging Investigative Technologies.

AUDIT OBJECTIVE AND SCOPE

The objective of the audit was to determine if the RCMP has the governance, internal control and risk management frameworks in place to support the adoption, integration, and use of selected EIT. The scope of the audit examined whether a governance, decision-making, and oversight structure for EIT exists and how it operates at the organizational level. The audit also examined whether a comprehensive approach exists to acquire and manage specific EIT used within the RCMP. The specific technologies scoped in were RPAS, investigative genetic genealogy technique (IGGT), and St. ROCH (RCMP Operational Centralized Holdings). The time period in scope was from April 1, 2019 to December 31, 2021.

This audit did not examine Body-worn cameras. The RCMP Body Worn Camera Performance Measurement and Evaluation Plan was conducted by National Program Evaluation Services in 2021. An agile audit of BWC was initiated in 2022-23, and additional audit work is planned in the two years post deployment of BWC. [REDACTED]

FINDINGS

The following aspects of the framework to adopt and manage EIT require management's consideration. The detailed observations and recommendations are discussed further in the report.

Observation 1: There is an incomplete approach to addressing governance related to EIT. It is fragmented, and focuses on higher dollar priority projects/ initiatives.

Observation 2: The development of a comprehensive approach to IGGT is ongoing; however, opportunities exist for interim guidance on the planning, acquisition and use of IGGT in the RCMP.

Observation 3: A comprehensive approach is in place to guide the planning, acquisition and use of RPAS in the RCMP. However, opportunities for improvement exist related to privacy, transparency and data protection.

Observation 4: A comprehensive approach is in place to guide the planning, design, implementation and management of the St. ROCH Project. As St. ROCH evolves into the program state and beyond, ongoing assessment of privacy considerations and AI will be key.

OVERALL AUDIT OPINION

At an organizational level, governance exists for higher value EIT projects, however there is an incomplete approach to addressing governance related to EIT as a whole. The frameworks in place to support the adoption, integrations and use of the three EIT examined in this audit were at different stages of maturity. Some opportunities for improvement exist.

From a risk management and internal control perspective, there are potential risks related to privacy and IM when contracting with third-parties. There is an opportunity for Policy Centres responsible for specific EIT to assess and mitigate these risks through consultation with Departmental Security (DS), the IM/IT Program, Procurement and other relevant subject-matter experts (SMEs).

NEXT STEPS

The management response and action plan developed in response to this report demonstrate the commitment from senior management to address the audit findings and recommendations. RCMP Internal Audit will monitor the implementation of the management action plan (MAP) and undertake a follow-up audit if warranted.

MANAGEMENT'S RESPONSES

Specialized Policing Services (SPS) supports the findings of this audit report. The RCMP has and must continue to adapt to emerging technologies. Additional resources, as well as operations and maintenance funding, would be required to fully implement these recommendations, and to continue building capacity and capability across the organization in support of policing operations

Bryan Larkin
Deputy Commissioner, Specialized Policing Services

Overall, Contact and Indigenous Policing (C&IP) is supportive of the findings and recommendations in the Audit of Emerging Investigative Technologies report. C&IP will work collaboratively with all business lines to develop a detailed action plan to address the findings and contribute to the RCMP's adaptability in emerging investigative technologies. Further, C&IP will require additional resources and funding to successfully implement any of the recommendations outlined in this report.

Brian Brennan,
Deputy Commissioner, Contract & Indigenous Policing

Federal Policing agrees with the audit's findings and is supportive that the organization requires a coordinated organizational effort to develop appropriate committee oversight, policy frameworks, and standardized processes for assessing/adopting EIT, especially given that the recommendations all have organizational implications.

In relation to the governance of EIT, and as highlighted in the audit, there is a governance structure for the St. ROCH which will remain. We agree that an EIT organization framework should be implemented to assess, adopt and monitor EIT, especially of lower dollar value tools. The program recognizes the importance of a governance framework to mitigate potential issues to ensure data is collected lawfully and accurately.

The St. ROCH program has hired a Privacy Impact Assessment (PIA) specialist to work with the RCMP Access to Information and Privacy (ATIP) Branch to deliver a PIA for Federal Policing. The St. ROCH program has implemented the Model Manager and Algorithmic Impact Assessment (AIA) framework necessary to meet the TB automated decision-making requirements. These oversight and accompanying controls (guidelines, standard monitoring procedures, training, policy and monitoring) are being implemented and will be in place once the platform goes live in the next fiscal year. As we get closer to the fall of 2024, a communication strategy will be put in place internally and externally to ensure transparency in relation to our capabilities.

Michael Duheme
Deputy Commissioner, Federal Policing

Overall, Corporate Management & Comptrollership (CM&C) agrees with the findings and recommendations in the Audit of Emerging Investigative Technologies report and supports the areas identified for improvement, particularly in regards to Governance for projects and new investments. CM&C will work with the appropriate Policy Centers to support the development of a detailed action plan to address the report recommendations, including specific timelines and milestones.

Samantha Hazen,
Chief Financial Officer

1 BACKGROUND

1.1 AUDIT CONTEXT

The RCMP's 2020 Environmental Scan identified that the world is undergoing a fourth industrial revolution whereby innovation is driving the emergence of new technologies at unprecedented rates, and individuals are gaining expanded access to these advancements. Technology is becoming increasingly connected, merging the digital and physical realms in new ways that uniquely enable both law enforcement and criminality.

While these innovations have resulted in tech-savvy criminals driving the increase of technology-based crimes, emerging technologies also provide law enforcement with new methods and means to investigate and prevent crime, increase employee and public safety, and improve access to information for timely decision-making.

Emerging investigative technology is a concept without a formal definition in TB policies or the RCMP. EIT used by law enforcement can encompass:

- Physical equipment, such as automatic licence plate readers, RPAS, and BWC,
- IM/IT tools or software such as media aggregation tools, AI and ML, decryption tools and on-device investigative tools,
- Forensic science-driven technologies such as genetic genealogy, genetic profiling, biometrics (facial and voice recognition).

EIT can be a good purchased off the shelf, a technology developed in-house, or a service acquired through a third party.

Due to the speed at which these new investigative technologies emerge and the relative ease by which they can be publicly acquired and accessed, many are not yet governed by legislation or policies.

This audit is intended to support the RCMP in achieving its modernization objectives related to operational tools, equipment and technologies, which is a priority identified in Vision 150 and Beyond: RCMP Strategic Plan. For these reasons, the RCMP Risk-Based Audit and Evaluation Plan 2021-2026 included the Audit of Emerging Investigative Technologies.

2 OBJECTIVE, SCOPE AND METHODOLOGY

2.1 OBJECTIVE

The objective of the audit was to determine if the RCMP has the governance, internal control and risk management frameworks in place to support the adoption, integration, and use of selected EIT.

2.2 SCOPE

The scope of the audit examined whether a governance, decision-making, and oversight structure for EIT exists and how it operates at the organizational level. The audit also examined whether a comprehensive approach exists to acquire and manage specific EIT used within the RCMP. The specific technologies scoped in were RPAS, IGGT, and St. ROCH. The time period in scope was from April 1, 2019 to December 31, 2021.

This audit did not examine BWCs. The RCMP Body Worn Camera Performance Measurement and Evaluation Plan was conducted by National Program Evaluation Services in 2021. An agile audit of BWC was initiated in for 2022-23, and additional audit work is planned in the two years post deployment of BWC. The use of [REDACTED] facial recognition tools was also excluded due to legal proceedings associated with it.

2.3 METHODOLOGY

The audit was conducted between November 2021 and October 2022. The audit team employed various techniques including file reviews, interviews, walkthroughs, and review and analysis of supporting documentation. With the exception of the St. ROCH case study, the audit was conducted remotely, via video-interviews and electronic submissions of supporting evidence, due to travel restrictions related to the COVID-19 pandemic.

Specifically, the audit team:

- Selected a sample of six divisions [REDACTED] to provide a geographically diverse perspective on the adoption and management of EIT.
- Conducted interviews with key personnel in [REDACTED] Divisions, as well as SPS, C&IP, Federal Policing and CM&C. These interviews included senior management in the divisions, investigators, National and Divisional RPAS coordinators and operators, policy centre personnel, key program staff and representatives of oversight committees.
- Reviewed documentation and supporting evidence to validate information provided in interviews and determine compliance with RCMP policy requirements.
- Completed a walkthrough of the St. ROCH system.

For the purposes of criterion 2 of the audit, EIT have been grouped into three categories: (1) equipment, (2) services provided by third parties, and (3) IM/IT, reflected in Table 1 below. Based on a risk assessment and planning interviews, one EIT per category was selected for assessment and case study. These are represented in blue in Table 1.

Table 1 – Categories of EIT

Equipment	Services (provided by 3rd party)	IM/IT (tools or software)
• Automatic License Plate Recognition • ShotSpotter • Remotely Piloted Aircraft Systems ("Drones") * • Sensors • Body-Worn Cameras • In-Car Video • Cell-Block Video • Cell-Site Simulators • X-Ray tools	• Investigative Genetic Genealogy Technique* • DNA Analysis • Cloud Services • Media Aggregation • Facial Reconstruction /3D scan • Genetic profiling Could also include services for items listed under Equipment and IM/IT	• Biometrics (facial, voice, DNA, prints, etc) • Artificial Intelligence • Decryption tools • Computer Forensics • AI/ Machine Learning • Multi Purpose Data Analytics • On-Device Investigative Tools • Android Team Awareness Kit • St. ROCH*

Detailed criteria are contained in Appendix A of this report.

2.4 STATEMENT OF CONFORMANCE

The audit engagement conforms to applicable standards in the Institute of Internal Auditor's International Professional Practices Framework and the Treasury Board of Canada Directive on Internal Audit, as supported by the results of the quality assurance and improvement program.

3 OBSERVATIONS

3.1 CONTEXT

Transformation in the RCMP

As the RCMP approaches its 150th anniversary in 2023, the organization's top priority is to be the modern, inclusive and healthy organization that its employees and all residents of Canada expect. To accomplish this, there are key initiatives underway in the 'Vision 150' strategy. Elements within these initiatives that are relevant to the Audit of EIT fall within two areas:

- **support modern policing**, which includes applying a Gender-Based Analysis Plus (GBA Plus) approach across the RCMP to help ensure that all of its policies, programs and processes are inclusive and help create a safer, healthier work environment for everyone, and
- **improving accountability and transparency**, which includes equipping officers with BWCs to improve public transparency and accountability and to respond to concerns about policing from racialized and Indigenous communities. A PIA for BWC is in progress, and once the RCMP internal policy to support the use of BWCs is completed, it will be posted on the RCMP website. Although BWC was not assessed within this audit, the accountability and transparency approach related to BWC could be applied to other EIT.

Outcomes from these two elements can be beneficial in moving forward the three EIT cases studies in this audit, as well as other EIT being used or considered for use within the RCMP.

Benchmarking

The audit team obtained benchmarking information to identify initiatives being undertaken by other police organizations related to the adoption and use of EIT, including the development of EIT policy, frameworks, and public consultation.

Policy Frameworks

The International Association of Chiefs of Police[1] (IACP) and the New Zealand Police[2] have developed similar policy frameworks and principles for trial or adoption of new policing technology. Some of the key principles were policy, privacy, transparency, public consultation, proportionality, data management and security, performance evaluation and accountability.

[1] International Association of Chiefs of Police, IACP Technology Policy Framework, January 2014
https://www.theiacp.org/sites/default/files/8.%20IACP%20Technology%20Policy%20Framework.pdf
[2] New Zealand Police, Trial or adoption of new policing technology, March 2022 (updated July 2022)
https://www.police.govt.nz/sites/default/files/publications/trial-or-adoption-new-policing-technology-130722.pdf
https://www.police.govt.nz/sites/default/files/publications/new-technology-framework.pdf

Transparency and Public Consultations

An increasing number of Canadian and foreign police agencies have taken specific measures to enhance transparency in their respective agencies' use of new technology, by notifying the public of the technology used, and when/how it can be used. In addition, most have also sought public input and feedback on the adoption of new technologies and related policies, as per Table 2 below.

Table 2– Police Services Transparency and Public Consultations

Police Service	Transparency and Public Consultations
Toronto Police Services Board	December 2021 - invited the public to submit feedback on a draft Policy[3] that would govern the way the Toronto Police Service could obtain and use new AI technologies. The Board was developing policy to create transparency about the Service's use of AI technology, and to ensure that AI technologies are used in a manner that is fair, equitable, and does not breach the privacy or other rights of members of the public.
Edmonton Police Service	In 2022 - published a media release[4] (including frequently asked questions) informing that they are using a facial recognition solution to assist in criminal investigations, and after extensive research into the benefits have secured a contract to implement a solution.
Ottawa Police Service	In 2022 - published a media release[5] advising that they identified the need for Unmanned Aerial Systems (UAS), and will be using them to assist in responding to calls for service for serious and fatal traffic collisions, missing persons, and other operational requirements. It includes questions and answers, and contact information for enquiries.
Peel Regional Police Service	In 2022 - published a media release[6] which includes frequently asked questions and advises that the objective of their Body-Worn Camera project is to improve overall community safety and well-being, and focuses on transparency, accountability and trust through the demonstration of their members' professionalism.

[3] https://tpsb.ca/consultations-and-publications/artificial-intelligence-policy-consultation
[4] https://www.edmontonpolice.ca/News/FacialRec
[5] https://www.ottawapolice.ca/en/safety-and-crime-prevention/unmanned-aerial-system.aspx#What-are-the-benefits-of-an-UAS (accessed June 27, 2022)
[6] https://www.peelpolice.ca/en/in-the-community/body-worn-cameras-faqs.aspx

Waterloo Regional Police Service	In 2022 - published numerous media releases related to EIT which included frequently asked questions and contact information. Examples include: • The launch of a pilot project to utilize Body Worn Video and In-Car Video technology; • A media release on Privacy & Technology which includes information on Body-Worn Video, Digital Evidence Management System, Remotely Piloted Vehicles, Device Extraction, Image Analytics, and Brief Cam, as well as frequently asked questions and contact information[7]. • Notification that they use an Aeryon SkyRanger (RPV) to assist with a variety of law enforcement functions, other applications of the RPV are reviewed on a case by case basis, and they have conducted a PIA in consultation with the Information and Privacy Commissioner of Ontario[8].
New York Police Department	Prior to the adoption of significant policy changes, the New York Police Department seeks feedback from the public[9]. For newly acquired technologies, the Department proposes a draft impact and use policy on this website at least 30 days prior to such use. The Department also provides addendums to impact and use policies where enhancements are acquired for a specific technology or the technology is used in a manner not previously disclosed. Examples of policies posted in 2021 included: • Unmanned aircraft systems impact and use policy; • Cell site simulators impact and use policy; • Media aggregation service impact and use policy; and • Social network analysis tool impact and use policy.

In addition, the Government of Canada's (GC) National Action Plan on Open Government, 2022-2024[10] and the House of Commons Report of the Standing Committee on Access to Information, Privacy and Ethics, October, 2022, titled Facial Recognition Technology and the Growing Power of Artificial Intelligence[11] have also focussed on increasing transparency, accountability and citizen participation. These are intended to improve governance and enhance public trust.

What Was Expected

Open Government publications highlight the importance of having a governance approach that focuses on transparency, accountability, integrity, and citizen participation. They also show the importance of having legislation for the acquisition and use EIT, completing PIAs and consultations with key stakeholders, including the Office of the Privacy Commissioner of Canada (OPC), before acquiring technology, and the need to enhance transparency and public notice.

[7] https://www.wrps.on.ca/en/about-us/video.aspx
[8] https://www.wrps.on.ca/en/about-us/remotely-piloted-vehicle.aspx
[9] https://www.nyc.gov/site/nypd/about/about-nypd/public-comment.page
[10] https://open.canada.ca/en/content/national-action-plan-open-government
[11] https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/report-6/

Other police organizations have demonstrated efforts to increase transparency and public trust. The RCMP has made gains starting with BWCs, and can continue to modernize its operations to improve public transparency.

The RCMP Commissioner's direction to Commanding Officers in May 2022 stated that: "Looking to the future, we must make sure that benefits of any technology we use operationally are in balance with the rights and expectations of Canadians. To do this, we must ensure that all new investigative technologies undergo a thorough evaluation that assesses the privacy, legal, ethical and GBA Plus implications."

It is important that the RCMP is aligned with government-wide direction and developments within the police community. As such, Internal Audit expected the RCMP to have a framework in place that supports accountability and transparency for the adoption, integration and use of EIT.

3.2 GOVERNANCE

Observation 1: There is an incomplete approach to addressing governance related to EIT. It is fragmented, and focuses on higher dollar priority projects/ initiatives.

Governance enables the achievement of objectives, supports strategic decision-making, and management of risk. It provides organizational focus and directional alignment.

A network of national committees composed of RCMP senior executives from business lines exists within this organizational structure. They consult, advise and make decisions, and/or provide oversight on subjects that impact the RCMP's ability to achieve organizational objectives, and promote a consistent approach to policies, programs and services.

Duties such as oversight, strategic planning, decision-making and financial planning fall under governance activities.

EIT Governance Framework

Through interviews with senior stakeholders across the organization, the audit team found that there was no organizational framework or process in place to assess, adopt, integrate and monitor EIT. In general, units and divisions can acquire EIT locally based on their own needs and priorities.

Governance over EIT as a whole is fragmented. EIT cuts across established governance committees, but there is no single Tier 2 committee for EIT, as it potentially has implications for Operations, Policy, Investment Oversight, and Management committees. Governance exists for at least some high dollar value EIT projects, as evidenced by St. ROCH, but organizational gaps exist for lower dollar value EIT as evidenced by IGGT and RPAS case studies. The audit team also found that formal rules were not in place on how to use/monitor EIT, and there was a lack of tracking and monitoring. Monitoring that is done generally seems to be for high dollar EIT projects such as St. ROCH or BWCs. Risks and challenges identified in interviews included governance, roles and responsibilities, a lack of policy/ legislation, privacy/ transparency risks, and contracting/ data management risks.

Governance Committees

Key committees identified in interviews that may play a role in the adoption and integration of EIT included the Senior Executive Committee (SEC), the Operations Committee (reconstituted in January 2022 as the National Integrated Operations Council), the Committee on Digital Investments (CODI), the Investment Oversight and Prioritization Committee (IOPC), and the Committee for Assets & Materiel. Some of these committees were not active during the audit scope period. The revitalization of IOPC and CODI, the newer Data, Information and Analytics Committee and structures like the National Technologies Onboarding Program (NTOP) should assist in addressing gaps that have created risk for the organization.

Based on Records of Decisions (RODs), EIT was discussed primarily at the Operations Committee, IOPC, and CODI. However, discussions focused on high dollar value projects such as the St. ROCH Pilot, or organizational-wide initiatives such as the BWCs pilot project, and the Android Team Awareness Kit.

Interviewees noted that thresholds are not established for governance, and committees do not have visibility on all EIT. There is a lack of coordination between committees, and determining who needs to make decisions, e.g. SEC, Deputy Commissioners/Business line heads. Also, better coordination is needed between national and divisional governance. Divisions can feel compelled to adopt EIT independently because of the pace of national initiatives.

National Technology Onboarding Program

NTOP was developed by the RCMP Technical Operations Branch due to an absence of clear legislation on the use of investigative technology and the lack of RCMP standardized processes to onboard new technology. NTOP was formed in June 2021 to action the OPC recommendations[12] on the RCMP's previous use of facial recognition technology through [REDACTED] while building a program more general in scope to address all EIT.

NTOP's role is to create a framework to conduct assessments for onboarding technology. It will respond and promote the use of technology for operational needs through innovation or procurement; leverage internal technology experts and establish a standard evaluation framework; develop appropriate policy, legal and privacy frameworks; work with internal business lines to identify, assess, document, and safely deploy new tools and techniques; track the tool/technology through management of a centralized inventory; and, be transparent about how and when the RCMP is using technology starting with a clear operational need and public benefit. The NTOP lens will encompass EIT with the view of Legal, Ethics, Privacy, GBA Plus, Equity, Diversity and Inclusion (EDI), Risks, and Bias.

The possibility of NTOP conducting PIAs for the organization has been discussed at SEC, but will be dependent on funding. At the time of the audit, NTOP was not fully funded, there was no established framework, policy or procedures, and the involvement of NTOP was not mandatory in the assessment of EIT. In May 2022, the Commissioner directed Commanding Officers that anyone considering using any new operational technology needs to consult NTOP. The breadth and depth of subject matter expertise provided through NTOP will be important to its success, as will continued organizational buy-in.

Interviewees advised that although NTOP's role is significant, divisions are usually considering immediate technology needs and not necessarily thinking of where NTOP can take them.

Roles and Responsibilities

At the organizational level, roles and responsibilities are not clear relating to the adoption and integration of EIT. The organization has not clarified whether EIT falls under Cybercrime, Technical Operations, Federal Policing or the IM/IT Program. There is no single owner for EIT as a whole, rather it is dispersed across business lines and divisions according to the type of technology and user needs.

In general, units and divisions acquire EIT based on their own needs and priorities. The framework for the three EITs assessed as part of this audit were at different stages of maturity during the audit. The RPAS policy exists and includes roles and responsibilities, but was under revision. The IGGT policy is under development so is not finalized or published. The St. ROCH policy will be developed at a later stage in the project.

Interviewees stated that there is a lack of knowledge on available technology and what is being used, and no centralized mechanism to identify duplication or gaps. Each division has been implementing their own solutions,

[12] https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/

but the process could be streamlined to assist in identifying what technology is used by divisions and monitor its performance.

The RCMP's Action Innovation & Modernization unit provides guidance on the GBA Plus process, but does not have the resources or subject matter expertise to conduct GBA Plus analysis on EIT. They stated that possibly NTOP could include this activity in their processes. The RCMP's ATIP Branch provides advice and guidance on privacy considerations and PIA requirements, but cannot write the PIAs for program areas as that would be a conflict of interest. The Professional Responsibility Sector, which is responsible for organizational ethics, does not have any role or responsibility in the adoption or use of EIT.

Prioritization

At the time of the audit, there was no EIT prioritization process. There is a need to identify a single/or appropriate executive level committee to make EIT prioritization decisions. Currently, the prioritization of EIT projects with material value or high impacts can occur through different committees that feed into IOPC, e.g. CODI, Real Property Advisory Committee, Committee for Assets and Materiel, and Corporate Systems Investment Committee. Requirements are scored through a prioritization matrix, and IOPC considers the whole population to create the Investment Plan. If government priorities are linked to policy objectives and/or on mandate commitments, they may advance the line in CODI's queue. When priorities are identified, new priorities can displace previous ones due to limited human resources, and others may be put on hold.

Prioritization is largely funding-driven, and divisional and national priorities are not always aligned. CODI RODs noted discussion on project funding and prioritization, and in particular that real-time prioritization and better coordination among Tier 3 committees is needed to support and enhance the prioritization framework tool currently in place.

At the divisional level, EIT purchases may be brought to the division Equipment Committee, and EIT acquisition is prioritized by the Commanding Officer or Criminal Operations Officer (CROPS).

At the time of the audit, cost was the threshold for risk, and low dollar contracts did not meet the threshold for National Headquarters Procurement review. EIT can be identified/ approved, but top priorities are not always funded.

There is an opportunity for SEC to start focusing on the Tier 2 unfunded priorities. It is important that SEC is aware of the complete requirements. Processes are reactionary and budget proposals need to be developed.

Transparency

The audit team found that there has been limited transparency and Public Notice related to the RCMP's use of EIT. There have been instances where divisions have informed the media after the fact of successful EIT use (e.g. IGGT that identified human remains in historical cases). However, the majority of media and OPC attention relates to instances of the RCMP using EIT without informing the public, highlighting privacy concerns. An organizational approach to transparency in the RCMP's use of EIT could help enhance public trust and confidence and advance RCMP Modernization.

In October 2022, C&IP announced that the RCMP intends to proactively share information on its upcoming BWC usage and policy.

Conclusion Governance

Organizational governance over EIT that does not meet high dollar value thresholds could be strengthened. NTOP can play an important role in providing operational guidance on effective and responsible use of EIT from a personal information collection perspective.

There has been limited transparency and Public Notice related to the RCMP's use of EIT, such as proactive media releases on how/when/where certain EIT is used, and, when possible, sharing draft policy with stakeholders and the public for consultation. This should be increased to the extent possible to align with other police force practices and Open Government transparency initiatives.

Why these findings are important

Investments in technological advancements are being made to assist in operations and contribute to the success of the RCMP's mission of preserving the peace, upholding the law and providing quality service in partnership with communities across Canada.

The benefit of using IGGT, RPAS, St. ROCH, and other EIT continues to expand, as does public scrutiny over their use in relation to privacy. Public trust and confidence can be at risk if law enforcement's use of EIT is seen as unjustifiably intrusive or infringing on individual rights and freedoms.

A strong governance framework over EIT, including committee oversight, policy frameworks, and the standardization of processes to assess, adopt and use EIT, is necessary to support the organization in meeting its operational needs, while balancing privacy and transparency expectations.

Areas requiring management attention

- Development of an overarching EIT policy, including roles and responsibilities.
- Standardization of processes for the assessment, adoption on use of EIT, through required involvement by NTOP.
- An organizational approach to transparency for the RCMP's adoption and use of EIT.
- An organizational approach to address privacy implications related to the RCMP's adoption and use of EIT, including PIAs.

3.3 ACQUISITION AND MANAGEMENT OF SELECT EITS

3.3.1 CASE STUDY 1 – INVESTIGATIVE GENETIC GENEALOGY TECHNIQUE

Observation 2: The development of a comprehensive approach to IGGT is ongoing; however, opportunities exist for interim guidance on the planning, acquisition and use of IGGT in the RCMP.

IGGT is a process in which the Deoxyribonucleic acid (DNA) profile from an unidentified contributor of a bodily substance sample is compared against known DNA profiles held on commercial genetic genealogy databases.

This combination of DNA analysis and genealogical research helps form conclusions about the biological relatedness of people.

In law enforcement, the purpose of IGGT is to:

- identify either the contributor or a biological relative of the contributor;
- generate new investigative leads; and
- assist in identifying potential suspects or persons of interest.

Currently the *DNA Identification Act* does not address IGGT or other DNA techniques and DNA profiles not included in the National DNA Databank (NDDB) indices. In addition, the RCMP currently does not have IGGT expertise, resources, or the required advanced forensic technologies to perform the type of DNA analysis or genealogy investigation for IGGT. Therefore, these services are acquired as and when needed from private laboratories located outside of Canada. Initial IGGT services include DNA extraction, development of DNA profile, comparison to a public DNA databank (which permits law enforcement to conduct searches related to serious crimes), and a pre-set number of genealogy research hours. Some of these private laboratories offering IGGT services perform all the steps of the process, while others contract out certain portions.

While results of the initial IGGT process may be sufficient to help identify the contributor, in other cases they may only point to very distant biological relatives. As such, it may be necessary to purchase additional genealogy research hours or pay to compare the DNA profile to other public DNA databanks, both of which increase initial costs. Once a person of interest, suspect or biological relative is identified through IGGT, direct DNA comparisons must then be completed by RCMP laboratories.

The RCMP has used IGGT in historical homicides and unidentified human remains (UHR) cases when:

- all investigative avenues and leads had been exhausted,
- comparisons to the NDDB indices yielded negative results,

- comparisons to foreign missing person databases (in cases of UHR) yielded negative results, or were not possible,
- witness pools were shrinking given the passing of time, and,
- evidence was degrading.

Interviewees in [REDACTED] divisions identified [REDACTED] cases that used IGGT and [REDACTED] for which its use was being considered. RCMP units have been purchasing IGGT services primarily by acquisition card, or in a few instances by paying invoices through the RCMP's financial system.

Policy Framework

Currently, there is no legislative framework for IGGT. The *DNA Identification Act* predates this technique and at the time of the audit, no cases using IGGT had been tested in Canadian courts. However, an organization-wide framework or approach for the usage of IGGT, led by C&IP's National Office of Investigative Standards and Practices (NOISP) is under development. [REDACTED] Divisional policies have not been developed given limited use of IGGT and pending national policy.

Instances of IGGT use are not being reported, tracked or monitored, therefore the RCMP cannot confirm how many times, by whom and for what purposes IGGT was used. Based on interviews, documentation and RCMP financial data reviewed, the audit team estimates that IGGT was likely used [REDACTED] by [REDACTED] divisions included in the case study.

While the RCMP does not have IGGT expertise or training, these can be obtained from external laboratories and service providers. To date, limited training on forensic genealogy research has been provided to some RCMP analysts, but this expertise has not yet been developed in-house.

Impact Assessments

In a Globe and Mail article[13] dated December 6, 2020, the OPC was quoted as saying that they had not received a PIA from the RCMP for IGGT and had subsequently requested that one be completed. The PIA questionnaire was completed by NOISP, and reviewed by the RCMP's ATIP Branch who requested a full PIA. However, at the time of the audit the PIA had not been started. In October 2022, NOISP advised that they were about to secure external resources to complete this and other PIAs within C&IP due to the lack of expertise in this field.

Currently, GBA Plus and EDI are not being considered for the individual case use of IGGT in the divisions, but policy centre interviewees indicated that they plan to integrate them into the PIA development process for IGGT.

Legal and Ethical Considerations

While there is no legislation governing IGGT, investigators are mindful of operating within the limits of (or not contravening) the *DNA Identification Act*, the *Privacy Act* and the *Canadian Charter of Human Rights and Freedoms.* Consultations with Crown attorneys occurs in some divisions for ongoing cases where they are analyzing suspect DNA, while other divisions can only approach Crown attorneys upon conclusion of investigations.

[13] https://www.theglobeandmail.com/canada/article-privacy-commissioner-calls-out-mounties-on-lack-of-dna-disclosures/

[REDACTED] Going forward, NOISP is proposing to have Divisional Legal Application Support Teams (LAST) involved, and to engage Crown Counsel for case-specific legal advice. Additionally, the draft RCMP IGGT policy states that GG results are not to be used to establish the sole or primary grounds to arrest a person, and serve as the primary evidence to lay criminal charges.

The types of investigations where IGGT is used adhere to the Major Case Management (MCM) investigative framework. Legal and ethical considerations are principles built into the MCM framework. Therefore, these considerations are already built into the investigative process for individual cases that ultimately proceed to using IGGT.

Transparency

Some transparency has been observed where divisional media releases have reported successful resolution of UHR cases where IGGT was used. However, from an organizational perspective, the RCMP has not proactively informed the public how/when IGGT is used, nor consulted key stakeholders who may be impacted by its use.

Procurement Practices

In lieu of formal acquisition documents or contracts, IGGT services are obtained following receipt of quotes for services via email, and paid for by acquisition card since the initial estimated costs fall well under the $10K threshold for acquiring services without a written contract. Approvals for the acquisition of IGGT services rest within the unit or may go up to divisional CROPS depending on financial authority limits. In the [REDACTED] cases reviewed, the audit team found appropriate supporting documents for IGGT transactions (quotes, invoices, credit card statements and logs), and that employees approving expenses (Section 32 and 34 *Financial Administration Act* [FAA]) had appropriate financial authorities. The only exception was that financial authorizations to incur the expenses (Section 32 FAA) were not documented in writing by the approver, but were relayed verbally to the investigative team.

For individual cases, costs may increase from the initial quote due to additional services purchased following results of initial DNA extraction/analysis and genealogy work. These add-on services may result in exceeding the $10K threshold for acquisition card purchases of services without written contracts. Another factor in exceeding financial thresholds is that the currency exchange rates applied on acquisition card purchases may not be considered by investigators when calculating estimated costs of using IGGT. Although they were outside our scope period, interviewees relayed that two instances of inadvertently exceeding the $10K threshold were flagged by Regional Corporate Management who required that they complete retroactive contracts and sole-sourcing justification forms.

Third-Party Risks

Currently, some forensic investigative techniques are not provided by the RCMP, such as IGGT, due to a lack of legislation and expertise, as well as, limited resources. As a result, investigators are using private laboratories to fill the gaps and help advance investigations.

Work completed by RCMP laboratories and private laboratories are mutually exclusive. Externally developed DNA profiles cannot be compared to the NDDB holdings, or vice versa, due to requirements in existing legislation. This creates risk of consumption of potentially limited DNA samples. In addition, a direct comparison would not be possible since IGGT examines different portions of the DNA compared to the conventional DNA analysis done by the RCMP laboratories.

Laboratories that perform GG or DNA extractions from degraded and/or fragmented samples are situated outside Canada (United States and Europe), and some also sub-contract portions of the work. Currently, security

requirements and protection of DNA data/information and exhibits have not been assessed in the acquisition of IGGT services from these foreign providers, which are governed by their own countries' laws and regulations. Because formal contracts are not currently being completed, there are no formal agreements addressing privacy, data and exhibit safeguards. Further, most interviewees did not indicate that consultation was occurring with RCMP Procurement and DS.

Conclusion IGGT

Due to the absence of legislation, framework and policy, there is a lack of guidance on how, when and for which types of cases IGGT can be used. As such, investigators are left to forge their own path in using IGGT, often by consulting peers, RCMP laboratories and IGGT service providers. Due to the lack of monitoring, the RCMP does not know the frequency of usage and cannot ensure that IGGT is being used appropriately. The draft IGGT policy is intended to address this gap.

There remains uncertainty and ambiguity relating to the legal, privacy and ethical implications of IGGT, given the lack of legislation, policy, and PIA. In addition, there is an opportunity for parameters to be set for GBA Plus and EDI considerations when using IGGT.

There is also opportunity for improvement where public notice could be given on the overall use of IGGT by the RCMP and for the consultation of key stakeholders that may be impacted by its use. A method similar to the recent approach used for the BWC initiative could also be applied to IGGT.

Procurement practices could be strengthened through consultation and training to avoid using improper purchasing methods, retroactive contracts, contract splitting and contravening sole-source purchase requirements. Data, information and exhibit management, security, and privacy protection have not been assessed, nor appropriate safeguards formalized in writing with foreign service providers.

Despite the lack of formal policy and guidance, investigators are being extremely cautious in the selection of cases for which to use IGGT and seldomly use it. They have seen the benefits and successes it brings to investigations, and they are aware that privacy and legislative risks remain. They are hopeful that the ability to use this technique will continue to bring closure to the families of victims and missing persons.

Why these findings are important

Framework, policy and guidance can help ensure that IGGT is used in approved circumstances by investigators, that the organization is able to track its usage and monitor that it is used appropriately. This is particularly important given the absence of legislation over IGGT.

Completion of a PIA can help ensure that programs and activities identify and mitigate negative impacts they may have on individuals' privacy and help build trust with Canadians by demonstrating due diligence and compliance with legal and policy requirements.

GBA Plus and EDI consideration are important to understand how diverse groups of women, men, and gender-diverse people will experience IGGT and to address or avoid inequalities and unintended impacts of using this technique.

Transparency and stakeholder engagement would improve accountability, transparency and demonstrate that the RCMP balances the benefits of using EIT in operations with the rights and expectations of Canadians.

Lastly, improper management, safeguarding and privacy protection related to data, information and exhibits could negatively affect investigations, breach the privacy of individuals and be non-compliant to legislation.

Areas requiring management attention

- Framework and policy for the assessment, adoption and use of IGGT
- Privacy, GBA Plus and EDI assessments
- Transparency and stakeholder engagement
- Procurement of services with third-parties located outside Canada, particularly in relation to:
    - Using procurement measures appropriate to the planned cost and in compliance with procurement policy,
    - Formalizing requirements, terms and conditions in writing,
    - Data/information/exhibit/privacy management, protection and security.

3.3.2 CASE STUDY 2 – REMOTELY PILOTED AIRCRAFT SYSTEMS

Observation 3: A comprehensive approach is in place to guide the planning, acquisition and use of RPAS in the RCMP. However, opportunities for improvement exist related to privacy, transparency and data protection.

A remotely piloted aircraft (RPA) is a power-driven aircraft with components, such as a camera, that is operated without a flight crew member on board. An RPAS is a set of configurable elements consisting of an RPA, its associated control station, the required command and control links, and any other system elements required during flight operation.

RPAS are also commonly referred to as drones, Small Unmanned Aircraft (SUA), Unmanned Aerial Vehicle (UAV), and Unmanned Aerial System (UAS). The RCMP's preferred terminology is RPAS.

Although RPAS have been in use in the RCMP for over 10 years, the RPAS program and capabilities were not rolled out uniformly in divisions, with some only acquiring their first RPAS in the last four years. RPAS are intended to capture an aerial account of events/incidents to support RCMP operations.

RPAS are used by the RCMP primarily for crime scene examination, forensic collision reconstruction, search and rescue, international border investigations, and monitoring critical incidents such as those involving Emergency Response Teams. They are used for surveillance purposes only with prior judicial authorization, or where urgent or exigent circumstances make it impractical to first obtain a search warrant.

Divisional RPAS Coordinators are responsible for the day to day operations of RPAS and provide advice to clients on their RPAS needs. Requests for operational drone services or for the purchase of drones funnel through them. The procurement of RPAS is decentralized, as most is undertaken divisionally on a case-by-case basis; however, approval from the National RPAS Program Manager is required for the procurement of new RPAS not currently in use by the RCMP. Led by C&IP, the National RPAS Program provides oversight and guidance, and is responsible for RPAS policy, the National RPAS Operations Manual, pilot flight logging, training, and the development/maintenance of RPAS standard operating procedures (SOPs) for divisions. RPAS use is also governed by Transport Canada regulations.

Policy Framework

A framework is in place for the adoption and use of RPAS, which includes Transport Canada's *Canadian Aviation Regulations* (CARs), RCMP RPAS Policy (Operational Manual 25.7), the National RPAS Operations Manual, SOPs and guidance from the National RPAS Program. Divisional policy supplements also exist, however there are some gaps in information because some pre-date national policy, or are not aligned/ linked to it.

The RCMP policies include requirements for RPAS pilot training, certification, pilot flight hours, and the maintenance of RPAS. Interviews and documentation provided indicates overall compliance, but there may be some challenges meeting the expected flight hours in policy. RCMP policy has more stringent expectations than

Transport Canada policy, which does not have any minimum requirement for flight hours, and informal provisions for reduced flight hours are in place pending the RCMP policy update.

Although the draft policy update has been developed, it is not expected to be published until after the revised PIA, which would prolong current gaps in information. [REDACTED]

Privacy

A PIA was completed in 2018 and the OPC provided concerns and recommendations that will be addressed in the pending PIA and RPAS policy updates, however the timeline for finalization has yet to be determined.

Outstanding issues identified in 2019 by the OPC include:

- the 2018 RPAS PIA provided an incomplete list of the personal information elements that RPAS may capture, such as a person's face, colour, body attributes or other particulars assigned to an individual, and,
- did not appropriately score the sensitivity of these elements, especially since images and videos are recorded in real time.

PIA updates are being led by C&IP's National Traffic Programs and Operational Technology, the RCMP's RPAS Policy Centre. [REDACTED]

There are gaps in definitions and understanding of AI and ML. As technology evolves, the RCMP may move toward the use of AI capabilities in RPAS. Although interviewees advised that they are not currently using AI capabilities, this is being considered, and as the RCMP moves in this direction, it could create risks related to GBA Plus, EDI, privacy and public perception of transparency.

Legal Considerations

Divisional RPAS Coordinators stay abreast of legal considerations for operating RPAS and are careful to ensure legal authority to operate drones. RPAS pilots follow national policy on use of drones (warranted or warrantless), and Divisional Coordinators encourage requesting units to speak with the divisional LAST for guidance on specific operations and use of warrants for them.

Information Management

There are potential IM gaps on the handling of RPAS Secure Digital (SD) card data, the transfer of information to investigators and the deletion of files from the SD card once saved to other media storage devices. Due to a lack of guidance within the RPAS policy on information management, and IM policy not having specific guidance on RPAS data management, lead investigators and RPAS users may not be aware of the IM requirements for data captured by RPAS.

There are gaps in security procedures for the collection, transmission, storage and disposal of personal information. Individual(s) in recordings could be compromised should the information be lost or mishandled. The impact of a breach includes liability, loss of credibility in the handling of personal information, compromising of criminal investigations, and financial loss to the organization if legal action is pursued. C&IP has advised that the policy update is expected to provide more specific guidance on these requirements.

Procurement Practices

Overall, the acquisition of RPAS adheres to accepted procurement practices, however there are some potential risks in the procurement process. Low dollar procurement does not meet the threshold for RCMP Procurement review, and there is potential risk related to how third-parties manage information captured by the RPAS through applications.

Procurement under $10K is often done by acquisition card, and procurement over $10K is done through Regional or National Procurement, or Public Services and Procurement Canada (PSPC). Divisional RPAS Coordinators assist clients in properly assessing RPAS needs, recognizing that top of the line and all accessories available are not necessarily required. The selection of the drones is based on what the client needs to accomplish for the success of missions. Divisions determine their own requirements for individual procurements, which are supported by research, business cases, consultation, and through approvals from the Divisional Coordinators, the National Program Manager, Officers in Charge of units and/or CROPs. Procurement spending limits (staying below $10K) and complex procurement processes (over $10K) were noted as challenges. Also, there were cases where obtaining management approval to purchase RPAS was difficult as they did not understand the benefit to the program.

In addition, there is a lack of consistency on whether RPAS contracts should be treated as IT and whether IT pre-approval is required. [REDACTED] divisions in the case study were following the IT Goods and Services Pre-Approval Request (Form 3868) process. Divisional Informatics Officer / IT Procurement sections across the organization were asked if RPAS is considered an IT technology/ asset and if a Form 3868 approval is required and most responses received [REDACTED] were no. Implications should be considered from an enterprise integration and asset management perspective.

Third-party risks

RPAS are often purchased from third party vendors outside of Canada, e.g., some of the RPAS purchased are manufactured in China (DJI). The application to operate the RPAS belongs to the third party, so it is possible that the application (app) could be recording and storing the data automatically. [REDACTED] Of note, DJI was blacklisted by the Pentagon on October 21st, 2022[14] due to National Security concerns. Although the Federal Bureau of Investigation and Department of Homeland Security acknowledged that they were continuing to purchase and use Chinese-made drones, they stressed that the agencies are attempting to move away from Chinese drones.

Some inconsistency was noted for approvals for purchasing for third party vendors. One division noted that requests are sometimes denied at the divisional level by DS although they are approved in other divisions, and another noted that some areas will not buy Chinese drones as they do not meet security requirements. [REDACTED]

Contracts over $10K do not include data and privacy protection clauses unless security requirements are identified. The contracts reviewed did not include data protection clauses, and most interviews did not indicate that procurement processes included consultation with the IM/IT Program and DS related to privacy and data safeguards. Procurement under $10K can be done without a written contract via an acquisition card. When using an acquisition card, there is nothing in writing that addresses how the vendor will manage RCMP data to which they may have access.

14 https://www.washingtonexaminer.com/policy/defense-national-security/drone-maker-fbi-dhs-chinese-military-company-pentagon

GBA Plus and EDI considerations

Although GBA Plus and EDI are considered for high dollar projects in TB submissions and may be included in PIAs, they are not considered or integrated in the processes to acquire RPAS (under or over $10K). Interviewees stated that when procuring RPAS, they are looking for the best possible technology that will meet the mission. No GBA Plus, EDI or ethical considerations were observed in procurement files reviewed.

Conclusion RPAS

The framework for the adoption and management of RPAS is the most developed of the three EIT case studies included in this audit, in that policy is in place, a PIA was completed, and there is support and guidance from the National RPAS program and Divisional RPAS Coordinators. Although RPAS have been in use in the RCMP for over 10 years, the RPAS program and capabilities were not rolled out uniformly in divisions, with some only acquiring their first RPAS in the last four years.

Efforts are being made to address OPC concerns through the ongoing RPAS policy and pending PIA updates. [REDACTED]

Visibility on risk factors related to GBA Plus, EDI and transparency could be improved at the divisional level, and are not currently being considered.

Although RPAS procurement practices adhere with acceptable practices, some risks may exist related to potential third-party access to RCMP data captured by RPAS.

Why these findings are important

Contracting with third party vendors who may have access to RCMP data or live-streams could create the risk of privacy breaches and impact investigations.

GBA Plus, EDI, privacy, AI and transparency related to RPAS use should continue to be assessed to minimize legal risk and public mistrust.

The OPC opinion is highly respected by the public, and failure to address privacy concerns and OPC recommendations has and will continue to reflect negatively on the organization.

Areas requiring management attention

- RPAS PIA update.
- RPAS policy update addressing OPC recommendations.
- Divisional policy supplements should be updated as necessary to align with national RPAS policy.
- Consultation with DS, IM/IT Program, and CM&C regarding third party contracts and data safeguard requirements (both under and over $10K).
- Determination as to whether RPAS should be considered an IT asset and require the Form 3868 approval process.

3.3.3 CASE STUDY 3 – ST. ROCH

Observation 4: A comprehensive approach is in place to guide the planning, design, implementation and management of the St. ROCH Project. As St. ROCH evolves into the program state and beyond, ongoing assessment of privacy considerations and AI will be key.

St. ROCH is an IT platform developed to enable the RCMP to modernize its technical capabilities by deploying a secure, [REDACTED] platform [REDACTED] capable of dealing with the big data issues faced during core policing investigational services. [REDACTED]

St. ROCH is being developed using an enterprise-approach. It was initiated internally as a Pilot, then developed into a Project [REDACTED] and designed to eventually be a National Program [REDACTED] and thus available to all divisions, with Program State expected to be achieved in 2024.

Prior to St. ROCH, the RCMP did not possess a technical means to process and evaluate big data (structured, semi-structured, unstructured) seized within the lawful mandate of operational policing. To address this gap, the St. ROCH pilot project was initiated, and ran from April 2018 to September 2019. At the conclusion of the pilot, the RCMP developed the necessary infrastructure to support this analytical solution and assess its effectiveness. The pilot project demonstrated significant efficiencies in the processing of big data, but data sets that were tested were limited and did not represent the full extent of St. ROCH's operational capabilities. [REDACTED]

There are several examples where St. ROCH has been successfully used to date. For an investigation involving approximately 100,000 documents in different languages, St. ROCH was able to process and translate these documents in approximately 19 hours at no cost. Typically, translation services cost from $250 to $500 per page. Additionally, under normal conditions, to review the results of seized data for an investigative file could employ the use of 30 FTEs working over a period of eight weeks. St. ROCH was able to perform the same task at 0.5 GB/minute in 100 minutes. [REDACTED]

St. ROCH Project Management

The needs assessment conducted prior to, and during the St. ROCH Pilot stage considered and had thoroughly documented evidence of the suitability, funding, implementation planning, legal and ethical considerations, GBA Plus, as well as EDI considerations.

The Project is consistent with the RCMP's modernization agenda and Digital Policing Strategy, and following GC protocols for new IM/IT projects. A Project Management structure exists for the St. ROCH Project. Also included within the adoption and management framework documents was evidence of consultations with both internal and external partners, which included the Five Eyes community, Treasury Board Secretariat (TBS), and the OPC.

[REDACTED] Procurements involved PSPC and were part of a competitive process. The acquisition of St. ROCH components is aligned with specifications and standards, adheres to accepted procurement practices and project management principles.

Performance Standards were measured and reported for St. ROCH throughout its development, and continue to be measured as it moves from Project to Program State. Financial tracking is in place for St. ROCH.

All business and technical requirements for the Pilot as well as the infrastructure requirements for the Project phase have been completed. Technical specifications and software implementations are well developed.

At the time of the audit, St. ROCH was not in Program state. Accordingly, governance, policies, SOPs, training requirements, performance standards, continual assessment, and monitoring requirements, are still in development and require further effort. That said, there are considerations for operation and maintenance of St. ROCH in both present and future. The Project Team continues to make adjustments and are maintaining the system as it goes from Project phase to Program phase. There is continuous monitoring of GBA Plus, EDI, Legal and Ethical considerations as the system is being built. Residual risks have been identified and are monitored.

Information Management

An IM framework is in place for St. ROCH, which addresses collection, use, access, security, retention and disposal of collected data and information. In addition, maintenance programs and protocols have been established for St. ROCH.

The data ownership is associated to the files at a granular level when the data is entered into the system and is maintained through the lifecycle of the data. St. ROCH must verify that the data seized during the investigation meets the conditions of judicial authorizations and relies on the Digital Forensic Services within the RCMP Technical Investigation Services to ensure that the conditions are adhered to while the data is being processed.

Data and information on the systems is used in investigations and there are SOPs for the sharing of information. [REDACTED] Disposal of data and information is as per uniform crime reporting retention parameters and coding.

Privacy Impact Assessment

In 2019 the OPC provided guidance on the St. ROCH project, and advised that RCMP should continue liaising with RCMP ATIP Branch with respect to completion of a PIA, and complete one if necessary.

The audit team reviewed documented evidence of the consideration of whether or not it is necessary to complete the PIA and feedback from the OPC. In particular, the St. ROCH Project has previously consulted with RCMP ATIP and from that initial assessment they were under the impression that, within their context:

(1) There was no need for a PIA given that there will be no changes to Federal Policing information collected during lawful criminal investigations through less efficient processes;

(2) That PIAs are not completed on tools, but are only required if new data repositories are being built; and

(3) Existing Personal Information Banks will be leveraged, whereby the RCMP already has the authority to collect information related to investigational activities.

In lieu of a formal PIA, the RCMP has agreed to develop a Privacy Threat and Risk Assessment to account for any privacy concerns and appropriate mitigation efforts. And in addition, should it be later determined that a PIA must be developed, the RCMP will ensure completion prior to St. ROCH's full operationalization.

At the time of the audit, a decision had yet to be made on whether a PIA is necessary.

Algorithmic Impact Assessment

St. ROCH has been an early adopter of the AIA process. The St. ROCH team has been working with TBS over the last few years on the development of the AIA, which includes continuous assessment of machine learning and data models developed and in use during the pilot and project phases of St. ROCH. In addition, the completion of the AIA is stated as a factor in achievement of the goal of aligning with the GC Architectural Standards on data collection with GC Enterprise Architecture Review Board requirements. Data must be collected using ethical practices supporting appropriate citizen and business-centric use, through the execution of the RCMP's lawful mandate to protect Canadian citizens. This will require continued collaboration with TBS to draft the AIA, and to continually adapt and modify AIA as the process matures in the GC as per TBS policies.

The OPC has also advised that the RCMP should continue liaising collaborating with the TBS to draft an AIA, and continue monitoring the data models used in ML.

Transition from Project to Program State

As St. ROCH transitions from Project to Program state, risks may increase with the potential implications of the expanded user base and likely variation in local/division business practices with respect to use of the platform.

Training is still being developed, but it was noted that the project budget has accounted for the tools necessary to develop, deploy, maintain, and support St. ROCH, as well as significant developer and end user training through custom plans. At the time of the audit, a Training Needs Analysis Report had been completed for St. ROCH and approved by the Director of National Learning Services.

It will be important to exercise caution and continue monitoring the rollout with commensurate internal controls in place, such as policy, guidelines, training, SOPs and monitoring.

Conclusion St. ROCH

There is a comprehensive approach in place to guide the planning, design, implementation and management of the St. ROCH Project. As it evolves into program state and beyond, ongoing assessment of privacy and AI will be key.

The RCMP St. ROCH Project should continue liaising with RCMP ATIP Branch with respect to completion of a PIA, and complete one if deemed necessary.

Additionally, as advised by the OPC in 2019, the RCMP should continue liaising and collaborating with the TBS to draft an AIA, and continue monitoring the data models used in Machine Learning. This is especially important as St. ROCH evolves from Project to Program state, as well as monitoring new capabilities and functionalities.

With respect to policy development and training, all business and technical requirements for the Pilot as well as the infrastructure requirements for the Project phase have been completed. The RCMP should continue monitoring GBA Plus, EDI, legal and ethical and other risks as the system is being built. As the Project moves forward, and prior to divisional rollout via the Enterprise approach, there is a need to continue to develop policy, SOPs and rollout training.

Why these findings are important

In 2019 the OPC provided guidance on the St. ROCH project that the RCMP should continue liaising with RCMP ATIP Branch with respect to the completion of a PIA, and complete one if necessary. Without a PIA or AIA in place, potential privacy risks and/or AI and Machine Learning may not have been fully understood, identified and appropriate risk mitigations put in place.

As St. ROCH transitions from Project to Program State, risks may increase with potential implications of an expanded user base and the potential variation in local/division business practices with respect to use. The capabilities of this system are powerful, and potential data linkages created and access to massive amounts of data have their own inherent risks. As many of these linkages are made with machine learning and data science principles, there should be some requirement for human intervention in decision-making, as per human-in-the-loop AI models.

It will be important to exercise caution and continue monitoring the rollout with appropriate internal controls in place, including policy, guidelines, training, SOPs, and continued monitoring. In addition, as the St. ROCH platform evolves to include new capabilities and make new linkages, the requirement for ongoing monitoring will be essential to manage and mitigate risks.

Areas requiring management attention

- In consultation with RCMP ATIP Branch and the OPC, a decision should be made as to the necessity of completing a PIA.
- Completion of the AIA.
- Finalizing policy, training and SOPs prior to the rollout of St. ROCH to divisions.

4 OVERALL CONCLUSIONS

At an organizational level, governance exists for higher value EIT projects, however there is an incomplete approach to addressing governance related to EIT as a whole. The frameworks in place to support the adoption, integrations and use of the three EIT examined in this audit were at different stages of maturity. Some opportunities for improvement exist.

Organizational governance over EIT that does not meet high dollar value thresholds could be strengthened. NTOP can play an important role in providing operational guidance on effective and responsible use of EIT from a personal information collection perspective.

Additionally, the framework for the three EITs assessed were at different stages of maturity during the audit. Policy governing EIT does not exist at the organizational level, however RPAS policy is being updated, IGGT policy is under development and St. ROCH policy will be developed at a later stage in the project. PIAs for EIT are not completed/revised in a timely manner, or at all. Failure to complete PIAs and/or address recommendations from the OPC has and will continue to reflect negatively on the organization.

There has been limited transparency and Public Notice related to the RCMP's use of EIT, such as proactive media releases on how/when/where certain EIT is used, and, when possible, sharing draft policy with stakeholders and the public for consultation. This should be increased to the extent possible to align with other police force practices and Open Government transparency initiatives.

As technology advances are trending towards more AI capabilities, it is important that the RCMP identify the current or desired use of AI, and understand/manage potential risks in a law enforcement context.

There are potential risks related to privacy and information management when contracting with third-parties. There is an opportunity for Policy Centres responsible for specific EIT to assess and mitigate these risks through consultation with Departmental Security, the IM/IT Program, Procurement and other relevant SMEs.

Conclusions specific to IGGT and RPAS

Contracts or terms and agreements are not in place for IGGT, and RPAS contracts do not contain privacy protection clauses, both of which create potential privacy and information management risks. Furthermore, there was a lack of consultation with the IM/IT Program and DS regarding potential privacy and data risks related to the use of third-party vendors located outside of Canada.

The acquisition of IGGT and related add-on services create high potential for escalation of costs that exceed the $10K threshold. Finally, GBA Plus and EDI are not considered or integrated in needs assessment and procurement process.

5 WHY IT'S IMPORTANT

Investments in technological advancements are being made to assist in operations and contribute to the success of the RCMP's mission of preserving the peace, upholding the law and providing quality service in partnership with communities across Canada.

For example,

- IGGT has been used successfully in progressing historical homicide cases.
- RPAS provide a cost effective, viable, and timely alternative to helicopters or fixed wing aircraft as an investigative aid. Deploying RPAS has reduced risk to members during operations. They have been used successfully for traffic collisions and reconstruction, search and rescue, international border observation, and situational awareness in critical incidents.
- St. ROCH has filled a technology gap for efficiently processing big data seized within the lawful mandate of operational policing.

The benefit of using these and other EIT continues to expand, as does public scrutiny over their use in relation to privacy. Public trust and confidence can be at risk if law enforcement use of EIT is seen as unjustifiably intrusive or infringing on individual rights and freedoms.

A strong governance framework to support EIT is necessary in meeting operational needs, while balancing privacy and transparency expectations. Continued attention to privacy, GBA Plus, and EDI considerations of EIT can assist the RCMP advance Modernization. It can also facilitate the RCMP's transparency in the use of EIT, bolstering public trust and confidence.

6 RECOMMENDATIONS

Given the cross-cutting and multi-business line impacts of the recommendations below, Internal Audit encourages key stakeholders to collaborate in their response to provide a pan-RCMP management action plan to best address the findings and related risks. The ultimate objective is to strengthen the governance, internal control and risk management frameworks in place to support the adoption, integration, and use of emerging investigative technologies.

1.	To support governance and facilitate a standardized process for EIT, the RCMP should consider thresholds for the required involvement of NTOP in the assessment of operational use of EIT.
2.	a) To support the adoption, use and integration of EIT, the RCMP should consider developing an overarching EIT policy. b) In addition, the RCMP should develop, maintain and/or strengthen organizational policy on IGGT, RPAS and St. ROCH to address the gaps identified in the case studies.
3.	To support Modernization, the RCMP should consider adopting an organizational approach to address privacy implications related to the RCMP's adoption and use of EIT (including PIAs).
4.	To support Modernization, the RCMP should consider adopting an organizational approach to transparency, including Public Notice, for the RCMP's use of EIT, where appropriate.
5.	To reduce organizational risk related to data collection, use, retention and disposal, the RCMP should, in consultation with CM&C and DS, identify and address risks related to third-party service provider access to RCMP data, and address potential risks within contracts.

APPENDIX A – AUDIT OBJECTIVE AND CRITERIA

Objective: To determine if the RCMP has the governance, internal control and risk management frameworks in place to support the adoption, integration, and use of selected emerging investigative technologies.	**Criterion 1:** A governance, decision-making, and oversight structure for emerging investigative technologies exists.
	Criterion 2: A comprehensive approach exists to acquire and manage the three selected emerging investigative technologies.

APPENDIX B – MANAGEMENT ACTION PLAN

Given the cross-cutting and multi-business line impacts of the recommendations below, Internal Audit encourages key stakeholders to collaborate in their response to provide a pan-RCMP management action plan to best address the findings and related risks. The ultimate objective is to strengthen the governance, internal control and risk management frameworks in place to support the adoption, integration, and use of emerging investigative technologies.

Recommendations	Management Action Plan
1. To support governance and facilitate a standardized process for EIT, the RCMP should consider thresholds for the required involvement of NTOP in the assessment of operational use of EIT.	1. Agree. a) The RCMP will publish the "Onboarding of New Operational Technologies" policy (Operations Manual Chapter 56.1). This policy will: • establish thresholds and requirements for the involvement of NTOP[15] when any RCMP program areas are considering the use of new operational technologies; • include a definition for Operational Technologies; • require client programs to contact NTOP before using or acquiring any operational technology that will be used in support of police operations; and, • define roles and responsibilities for NTOP, ATIP, IM/IT and DS, to ensure that all required analyses are completed prior to a technology being recommended for operational implementation. Completion date: August 2023 Position Responsible: Executive Director, Technical Operations b) In discussion with RCMP senior management, a permanent source of funding will be identified for NTOP to stabilize operations and ensure the current mandate can be met.

[15] While NTOP is not an approval body, it has robust processes in place to coordinate with clients, service providers, and DS to review and advise on investigative technologies, tools, and/or techniques, complementing existing governance for investment approvals and authority to operate from DS and the IM/IT Program. Mitigation strategies are in place to address program areas that attempt to implement controversial technologies against the recommendation of NTOP. In such cases, completed risk assessments would require signature by the Assistant Commissioner at the client level, as well as by the Chief Security Officer of the RCMP.

	Completion date: March 2024 Position Responsible: Executive Director – Technical Operations c) For Federal Policing initiatives, St ROCH / Data Science will become the single point of contact for Federal Policing EITs as it relates to data analysis to streamline interactions for assessment with NTOP, ATIP, IM/IT and DS. The organization will continue to emphasize governance and oversight that takes into consideration operational needs, privacy, and disclosure. Completion date: March 2024 for the structure to be in place, governance will be ongoing. Position responsible: Director General Federal Policing Covert Operations (FPCO), Covert Operations, Open Source and Data Science
2. a) To support the adoption, use and integration of EIT, the RCMP should consider developing an over-arching EIT policy. b) In addition, the RCMP should develop, maintain and/or strengthen organizational policy on IGGT, RPAS and St. ROCH to address the gaps identified in the case studies.	2. Agree. a) The new overarching "Onboarding of New Operational Technologies" policy (Operations Manual Chapter 56.1) will be published imminently, and will establish a comprehensive policy for the evaluation, tracking and implementation of new operational technologies, including the roles of NTOP, ATIP, IM/IT and DS. Further, it delineates the thresholds and requirements of RCMP program areas considering new operational technologies. Completion date: August 2023 Position Responsible: Executive Director, Technical Operations b1) As it relates to the St ROCH Program: As the St. ROCH platform moves from project to program state, procedures will be put in place when [REDACTED]. The following will take place: 1. NTOP, ATIP, Legal Services and Crown prosecutors are engaged to ensure that legal and privacy impacts/issues are identified, considered and mitigated. Completion date: December 2023 to identify legal concerns and implement mitigation strategies. This activity will be ongoing / revisited as the legal landscape evolves. 2. Policies and procedures will be put in place and will take into consideration technical, privacy and legal aspects. Completion date: Initial directive, December 2023 to coincide with the initial release of the platform.

	3. An end-user working group has been established and will continue its work to ensure the capabilities will meet the needs and / or that changes will be made to ensure the needs are met. Completion date: December 2023 to coincide with the initial launch of the platform. This will be ongoing afterward to align with ongoing operational needs. 4. Procedures for data management will be put in place. Completion date: December 2024 5. Review / auditing processes will be established for proper assessment once the platform is operational. Completion date: December 2024 As the St. ROCH project unfolds, policies and procedure will be continuously updated. Overall Completion date for St. ROCH: Late 2023 to operationalize the platform, with some aforementioned initiatives ongoing. Position Responsible: Director General FPCO, Covert Operations, Open Source and Data Science b2) As it relates to RPAS: The RPAS program is in the process of being transferred from Traffic Services in Contract and Indigenous Policing to Air Services Branch (ASB) in SPS. Upon transfer of the program (est. summer 2023), ASB will begin a full assessment of program operations to identify existing best practices and challenges, and develop a comprehensive library of use cases for RPAS technologies. Concurrently, ASB will begin to align RPAS operations with those currently in place for the rest of the RCMP air fleet, including flight management, pilot training and proficiency, IM practices, and technological standardization. This work will include the evaluation and revision of existing national and divisional policies and privacy impact assessments, and the development of comprehensive new policy suites governing the acquisition and use of RPAS technologies. Completion date/Position Responsible: As RPAS will be moving to SPS, additional time will be required to understand and properly assign ownership of this recommendation. A decision will be

	made over the next three to six months, and discussed with the Departmental Audit Committee in Spring 2024. b3) As it relates to IGGT: A comprehensive draft IGGT policy has been developed and will be finalized and published once the PIA is completed. The National Office of Investigative Standards and Practices' (NOISP) position is that once consultation with NTOP is complete, the draft policy should be used to formulate an interim directive to be communicated to CROPS officers or be published as interim policy subject to revision once the PIA/OPC process is complete. IGGT completion date(s): 1. Interim IGGT Policy June 30, 2023. Work is underway to formulate an interim directive. 2. Establishment of IGGT working group July 31, 2023. 3. Interim measures to support the timeline of PIA completion: Distribution of interim policy in Fall 2023 to all CROPS offices; IGGT to become standing agenda item on the National Major Case Management Committee (meets quarterly); tracking of IGGT through RCMP records management system (PROS/BC-PRIME). 4. Completion of PIA September 30, 2024. Final Policy: December 2024 (dependent on the completion of the PIA). Completion date: December 2024 Position responsible: Director General, National Criminal Operations (NCROPS)
3. To support Modernization, the RCMP should consider adopting an organizational approach to address privacy implications related to the RCMP's adoption and use of EIT (including PIAs).	Agree. 3a) The RCMP will develop an approach for the consideration of privacy implications on new program and technologies. As use cases for every technology have the potential to vary considerably, how operational technologies are employed must be considered at the program level, and not based solely on the implications of the technology itself. The NTOP evaluation should be considered as a complimentary component of internal assessment at the program level undertaken as part of the development of privacy impacts assessments required by Treasury Board directives.

	Completion date/Position Responsible: As Access to Information and Privacy has recently moved under the Chief Information Officer, additional time will be required to understand and properly assign ownership of this recommendation. A decision will be made over the next three to six months, and discussed with the Departmental Audit Committee in Spring 2024. 3b) The St. ROCH program has hired a PIA specialist to work with the RCMP ATIP Branch to deliver a PIA for Federal Policing. Completion date: December 2024 Position responsible: Director General FPCO, Covert Operations, Open Source and Data Science 3c) ASB's work to align RPAS operations with those currently in place for the rest of the RCMP air fleet will include the evaluation and revision of the existing RPAS PIA. Completion date/Position Responsible: As RPAS will be moving to SPS, additional time will be required to understand and properly assign ownership of this recommendation. A decision will be made over the next three to six months, and discussed with the Departmental Audit Committee in Spring 2024. 3d) C&IP will procure the services of an external PIA consultant on a casual contract to conduct the PIA for IGGT. Unfortunately, the previous consultant was unable to complete the PIA before contract termination and NOISP has not been successful in using internal resources for the completion of the PIA. Completion date: The PIA will be completed by September 2024 with the support of a PIA contractor. Until completion, interim mitigation measures as articulated in MAP 2b3 will apply. Position responsible: Officer in Charge, NOISP
4. To support Modernization, the RCMP should consider adopting an organizational approach to transparency, including Public Notice, for the RCMP's use of EIT, where appropriate.	Agree. The RCMP is developing a Technology Transparency Strategy. The strategy will identify new engagement and transparency initiatives specific to operational technologies. This will include creating opportunities for broader engagement with external stakeholders and the public on RCMP use of emerging tools and techniques, potential use policies, and greater access to information about operational tools used to support investigations.

	RCMP Technical Operations is currently working on a new transparency-based deliverable, the intent of which is to produce an unclassified, public document (e.g., Operational Technology Library) on select operational technologies / techniques in use at the RCMP, which will in turn, foster greater public confidence and trust through responsible transparency. RPAS will be included in the first iteration of this document with the goal to include all operational technologies in a publicly-available Operational Technology Library. Transparency efforts must be mindful not to not harm the effectiveness of technology and techniques; however, appropriateness is key and must be carefully considered on a case-by-case basis. A communication strategy will be put in place internally and externally to ensure transparency in relation to St. ROCH's capabilities. Public notice will be given on the overall use of IGGT by the RCMP and for the consultation of key stakeholders that may be impacted by its use. There is much media attention regarding IGGT and acknowledging RCMP's judicious use of the technique will not undermine investigations, will display public transparency, and satisfy some of the media interest directed to the RCMP. Completion date: December 2023 Positions responsible: Executive Director, Technical Operations; Director General, FPCO Covert Operations, Open Source and Data Science, and Director General, NCROPS.
5. To reduce organizational risk related to data collection, use, retention and disposal, the RCMP should: in consultation with CM&C and DS, identify and address risks related to third-party service provider access to RCMP data, and address potential risks within contracts.	Agree. RCMP programs will continue to work with CM&C and DS to address evidence-based organizational risks related to data collection, use, retention and disposal. The St-ROCH/Data Science team will work with DS to complete the Security Assessment and Authorization Process to comply with all required security controls and obtain authority to operate within the next 9 months. The St-ROCH / Data Science team will work with NTOP, ATIP and the Office of the Privacy Commissioner to ensure privacy is considered in the retention and disposal of information/data.

	St-ROCH / Data Science will establish its own procedures and policies as it relates to its platform and will ensure it is aligned with current established practices. St-ROCH/Data Science will identify issues related to data collection, retention and disposal if they arise and will work with appropriate partners to identify risks and make appropriate changes to mitigate these risks. Completion date: December 2024 Positions responsible: Executive Director, Technical Operations; Director General, FPCO Covert Operations, Open Source and Data Science, and Director General, NCROPS.