Special Review of RCMP-Sinclair Contract

Final Report

June 2023

Access to Information Assessment

This report has been reviewed for potentially sensitive information. Where sensitive information has been removed, asterisks [***] appear; published information is UNCLASSIFIED.

Table of Contents

ACRONYMS

List of Acronyms Used	
AP	Acquisition Program
CTI	Counter Technical Intrusion
DOB	Departmental Oversight Branch
DOS	Designated Organizational Screening
DSB	Departmental Security Branch
ERS	Enhanced Reliability Screening
FA	Facility Access
FOCI	Foreign Ownership, Control or Influence
IAER	Internal Audit, Evaluation and Review
IM/IT	Information Management/Information Technology
INDU	Standing Committee on Industry and Technology
IT	Information Technology
NRS	National Radio Services
NSE	National Security Exception
PMAM	Procurement, Materiel and Asset Management
PSPC	Public Services and Procurement Canada
RF	Radio Frequency
RFSO	Request for Standing Offer
SCI	Supply Chain Integrity
SEC	Senior Executive Committee
SO	Standing Offer
SOR	Statement of Requirement
SOW	Statement of Work
SRCL	Security Requirement Check List
TA	Technical Authority
TBS	Treasury Board Secretariat

EXECUTIVE SUMMARY

BACKGROUND

Sinclair Technologies is a communications equipment company that designs and manufactures radio frequency (RF) equipment. Its parent company, Norsat International, was purchased by Chinese telecommunications firm Hytera Communications in 2017. The Chinese government owns approximately 10 percent of Hytera through an investment fund.

A Public Services and Procurement Canada (PSPC) standing offer (SO) with Sinclair Technologies for communications equipment drew media attention and political scrutiny in December 2022, due to the vendor's ties to the Chinese government. Following a request from the Public Safety Minister to examine specific aspects of the SO with Sinclair Technologies, the RCMP suspended the SO in December 2022, to review the manner in which it was awarded and to mitigate against potential risks.

Subsequent to this, the RCMP's Senior Executive Committee (SEC) requested that Internal Audit, Evaluation and Review (IAER) initiate a review of due diligence over the procurement and security processes for the SO and resulting contracts with Sinclair Technologies to ensure that sufficient security protocols and assessments were conducted, and to capture any applicable lessons learned.

REVIEW OBJECTIVE AND SCOPE

The objective of this review was to provide an independent assessment of the procurement and security processes (including requirements identification and security) leading to the PSPC SO and RCMP contracts with Sinclair Technologies for RF and other equipment to ensure due diligence was conducted and that appropriate safeguards were taken. Evidence of any applicable lessons learned will also be reviewed and captured. The review included elements and actions within the authorities, processes and management of the RCMP.

The review assessed the processes leading up to the SO issued to Sinclair Technologies to procure RF and other equipment and the resulting three call-ups in 2021 and 2022[1]. In addition, the review focused on the elements within the control of the RCMP only.

OVERALL OBSERVATIONS AND CONCLUSION

The RCMP complied with applicable policies and procedures to establish the Sinclair Technologies SO for RF filtration equipment. Although subject matter experts confirmed that the equipment in this SO is low risk and does not compromise secure communications based on the RCMP's application, some lessons learned and opportunities for improvement exist to enhance the consideration and articulation of security requirements in procurement processes going forward. While addressing these areas will require collaboration with central agencies and other departments, the RCMP should develop guidance and/or implement controls to ensure RCMP security requirements are included in contracts, to address

[1] SO number M7594-210528/001/HN & Call-up #s 7255017, 7260562, and 7257258

security gaps around the Security Requirement Check List (SRCL) and to determine when additional security controls are necessary.

NEXT STEPS

The management response and action plan developed in response to this review 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.

MANAGEMENT'S RESPONSE

Corporate Management and Comptrollership supports the findings of this special review. The RCMP has robust governance and oversight structure that are in line with requirements of the Treasury Board Secretariat procurement policy suite. We will continue to comply with applicable policies and procedures. We are committed to collaborating with internal and external stakeholders to further strengthen procedures to keep Canadians and Canadian interests safe and secure in procurement practices.

Samantha Hazen, Chief Financial Officer

Specialized Policing Services supports the findings of this special review. The RCMP has rigorous screening procedures in place to keep Canadians and Canadian interests safe and secure. We will continue to comply with applicable policies and procedures, and will work with internal and external stakeholders on the report's findings, as authority on these matters will ultimately rest with Public Services and Procurement Canada.

Bryan Larkin, Deputy Commissioner, Specialized Policing Services

1 BACKGROUND

1.1 CONTEXT

Sinclair Technologies is a communications equipment company that designs and manufactures radio frequency equipment. Its parent company, Norsat International, was purchased by Chinese telecommunications firm Hytera Communications in 2017. The Chinese government owns approximately 10 percent of Hytera through an investment fund.

In October 2021, Public Services and Procurement Canada (PSPC) issued a standing offer (SO) on behalf of the RCMP with Sinclair Technologies, with an estimated potential usage of $550K to procure radio frequency (RF) equipment.[2] Appendix A provides additional information on the RF equipment.

The RCMP-Sinclair Technologies SO to purchase communications equipment drew media attention and political scrutiny in December 2022, due to the vendor's ties to the Chinese government. Following a request from the Public Safety Minister to examine specific aspects of the SO with Sinclair Technologies, the RCMP suspended the SO in December 2022, to review the manner in which it was awarded and to mitigate against potential risks.

Subsequent to this, the RCMP's Senior Executive Committee (SEC) requested that Internal Audit, Evaluation and Review (IAER) initiate a review as an extra layer of diligence and to seek an independent perspective over the procurement and security processes for the SO and resulting contracts with Sinclair Technologies to ensure that sufficient security protocols and assessments were conducted, and to capture any applicable lessons learned. The RCMP's National Radio Services (NRS) and Counter Technical Intrusion (CTI) conducted an inspection and technical testing on a recently acquired Sinclair radio frequency filter system resulting in no security concerns found. IAER reviewed the report and results; however, due to the specialized technical requirements of this testing, IAER did not have the expertise to independently verify the results of the NRS inspection and testing. In December 2022, Departmental Security Branch (DSB) consulted with Communications Security Establishment and received an opinion that RF filtering devices would not compromise encrypted communications based on the RCMP's application. Further, the RCMP was invited to appear before the parliamentary Standing Committee on Industry and Technology (INDU) on January 30, 2023, where the Chief Financial Officer and Deputy Commissioner of Specialized Policing Services responded to questions related to the contract awarded to Sinclair Technologies.[3]

1.2 OBJECTIVE

The objective of this review was to provide an independent assessment of the procurement and security processes (including requirements identification and security) leading to the PSPC SO and RCMP contracts with Sinclair Technologies for RF and other equipment to ensure due diligence was conducted and that appropriate safeguards were taken. Evidence of any applicable lessons learned will also be

[2] RCMP suspends contract with China-linked company | CBC News
[3] INDU - Contract Awarded to Sinclair Technologies (ourcommons.ca)

reviewed and captured. The review included elements and actions within the authorities, processes and management of the RCMP.

1.3 SCOPE

The review assessed the processes leading up to the SO issued to Sinclair Technologies to procure RF and other equipment and the resulting three call-ups in 2021 and 2022.[4] In addition, the review focused on the elements within the control of the RCMP only.

1.4 METHODOLOGY

The review of the Sinclair RF equipment procurement was conducted in three phases: planning, examination and reporting.

The planning phase of the review consisted of meetings with key senior executives to launch the review, development of the engagement Terms of Reference, collection of initial documents from clients, and formulation of Lines of Enquiry for the examination phase. This phase included research and consultation on applicable internal and external policies and procedures.

The examination phase included a review of relevant documents within the procurement file and interviews with key business lines involved with the procurement process leading to the SO with Sinclair Technologies. This included subject matter experts within:

- RCMP NRS
- RCMP Procurement, Materiel and Asset Management (PMAM)
- RCMP DSB
- PSPC Departmental Oversight Branch (DOB)
- PSPC Acquisitions Program (AP)

Finally, the reporting phase consisted of the drafting of the final report and consultation of stakeholders for fact validation.

1.5 STATEMENT OF CONFORMANCE

The review 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.

[4] SO number M7594-210528/001/HN & Call-up #s 7255017, 7260562, and 7257258

2 OVERVIEW OF THE PROCUREMENT PROCESS

2.1 PROCUREMENT INITIATION

The procurement process at the RCMP begins when a need is identified by an RCMP business line. Subject matter experts within the department, referred to as Technical Authorities (TAs) determine the technical and security requirements for the procurement. The TA identifies the specific technical requirements for the goods and services needed, which are documented in a Statement of Requirement (SOR) or Statement of Work (SOW). The TA sends a procurement package to PMAM to initiate the request, which includes the SOR/SOW, a requisition form, a Security Requirements Check List (SRCL) and an Information Technology (IT) Goods and Services Pre-Approval Request for goods or services deemed to be IT. The PMAM procurement officer assigned to the file determines the appropriate contracting strategy or vehicle for the procurement. Procurements that are above the RCMP's authority are delegated to PSPC as the Contracting Authority. PSPC reviews the documentation submitted, and consults with the RCMP Procurement Officer and the TA to clarify the requirements and obtain further documentation as needed.

2.2 SECURITY ASSESSMENT

Security requirements are assessed at the beginning of the procurement process. This begins with the TA assessing the risks by completing the SRCL, which is a key document to identify security requirements. The SRCL and related procurement documents are reviewed by the RCMP DSB, taking into consideration personnel, Information Management and Information Technology (IM/IT) and physical security risks, and makes recommendations on the required level of security. If DSB recommends security requirements, they provide a security guide to PMAM which includes details of security controls to be met by the supplier during the delivery of a contract. If no security requirements are identified, the requisition forms would indicate "no security requirements" and there would be no security provisions in the contract. The completed SRCL is signed by PMAM, DSB and the TA and included in the procurement package provided to PSPC if it acts as the Contracting Authority. If security requirements are identified on the SRCL for a procurement which PSPC manages, PSPC DOB performs a review of the SRCL, along with the associated SOR/SOW and any other relevant security companion to the SRCL and may recommend different or additional security controls, consistent with its lead security agency mandate. PSPC DOB will also release the required security clauses that must be included in the SO or the call-up (contract). After the security assessment process is completed, the procurement moves to the solicitation process.

Interviewees with DSB and PSPC noted that the SRCL form is from 2004 and that there are some gaps in the questions (e.g. cloud, cyber security and other sensitive aspects linked to national security which are not captured) and it could be more robust to assess modern risks in security. Also, it is used for all government departments, and does not capture some intricacies of RCMP security processes (discussed further in 3.2, below).

2.3 SOLICITATION, EVALUATION AND AWARD

At this stage, a method of supply is selected for the requirement. For some requirements, the preferred method of supply is a SO. In these instances, the procurement requirements are documented in a Request for Standing Offer (RFSO), which include instructions for bid submissions for potential vendors, the basis for evaluation, technical requirements and contract clauses. The RFSO is posted on the Government Electronic Tendering Service. When the bidding period closes, the RCMP TA evaluates the technical aspect of the bids to determine if they are compliant with the stated requirements, and PSPC evaluates the other aspects, such as pricing.

The SO is awarded to the vendor in accordance with the Basis of Selection detailed in the RFSO. Prior to awarding the SO, PSPC conducts an Integrity Regime check on procurements over $10K, as per PSPC's Ineligibility and Suspension Policy. This check involves determining if the vendor is suspended from or ineligible to be awarded the contract, based on being charged or convicted of an offense from a list of specific offences identified in the policy [5]. If no issues arise from the Integrity Regime check, the standing offer is awarded to the successful bidder. The SO is not a contract, it is an offer from a vendor to provide goods and/or services at pre-arranged prices, under set terms and conditions, when and if required. A contract is not in place until an authorized user[6] issues a "call-up" against the SO.[7]

2.4 CALL-UPS

A call-up against the SO is prepared to procure goods or services. The call-up needs to be compliant with requirements listed within the related SO, including eligible users of the SO, items listed, item pricing, labour pricing, and security requirements, if needed. Call-ups need to be done in accordance with an individual user's delegation of authority, which would usually be under $10K in the RCMP, with the exception of RCMP Procurement personnel.

Pursuant to the Financial Administration Act, Section 32 is confirmed on the requisition from the client, verifying that funds are available. Once the contract is fulfilled by the vendor and an invoice is received, Section 34 needs to be signed in accordance with the Financial Administration Act, which acknowledges goods and services were received in accordance with the contract.

[5] https://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html
[6] A SO will include a list of identified users within government department(s) who are authorized to make call-ups
[7] https://buyandsell.gc.ca/for-businesses/selling-to-the-government-of-canada/the-procurement-process/standing-offers#10

3 OBSERVATIONS AND RECOMMENDATIONS

3.1 COMPLIANCE

Overall, the RCMP was compliant with applicable policies and procedures to establish the SO; however, some lower risk issues were observed for one of the three call-ups.

The Review team performed testing to determine if the issuance of the SO and resulting call-ups (contracts) were compliant with relevant policy requirements within the scope of the review. It was determined that the RCMP followed the applicable requirements referenced in section 2. This included verification of the required procurement and security forms, approvals, and consultations. In addition, the Integrity Regime check was completed by PSPC.

Three RCMP call-ups were done prior to the suspension of the SO in December 2022, and these were assessed against policy and SO requirements. The activities surrounding two of the three were deemed by the review team as being fully compliant, whereas one call-up was deemed to be partially compliant, as some items purchased (valued at approximately $5,700.00) were not available in the SO appendices/ price lists. Call-ups need to be done in accordance with the SO, and as a result, these items should have been purchased separately. This was not considered a significant issue because these items were considered low risk and materiality, and could have been purchased independently of the SO under the delegated spending authority of individuals in Divisions or business lines.

While it is important that requirements specific to the SO are understood by users to ensure that Call-ups are compliant with its terms and conditions, no recommendations were warranted in the context of this review.

3.2 RCMP CONTRACT SECURITY

Security was considered by the RCMP as part of the procurement process. However, enhanced guidance and/or controls would be beneficial to ensure that security requirements specific to the RCMP are included in contracting documents and communicated to SO users and key stakeholders. Additionally, gaps related to RCMP requirements in the SRCL should be addressed and mitigating controls should be implemented until the SRCL is modernized by other government departments.

The review found that consultations had taken place between PMAM, DSB and NRS to determine what security requirements, if any, would be required for the 2021 Sinclair SO. Consultations between the RCMP and PSPC determined that there were no PSPC security requirements for the SO as none of the options within the SRCL were applicable for the RF filtration equipment. However, DSB determined that RCMP Facilities Access Level 2 (FA2) with an escort would be required, due to the potential for service providers to require access to RCMP facilities to perform services. FA screening is a type of security screening applied by the RCMP and is required by an individual whose duties or tasks require access to RCMP facilities. Individuals with FA status are not given access to protected or classified information, systems, assets or facilities. FA2 is an internal RCMP process, not security level on the SRCL or in the Treasury Board Secretariat (TBS) Standard on Security Screening. As a result, the SRCL was completed with no security requirements identified and the PSPC SO did not include any security requirements or clauses, with the RCMP solely responsible for any FA2 requirements. Interviews with RCMP and PSPC personnel noted that the SRCL form may not capture some intricacies of RCMP security processes, as it is used for all government departments. Interviews also indicated that the form is outdated. As a result, there may be an opportunity to review whether this form aligns with modern security requirements and ensure that mitigating controls are in place.

RCMP DSB conducted FA2 screenings, and clearances were granted to six Sinclair contractors in the event that work may be required on RCMP premises. To date, no on-site work has been required. However, the requirement for FA2 screening to be in place was not included in the SO and SOR, which could result in a lack of awareness of this requirement for RCMP personnel executing call-ups. This may increase the risk that intended security controls will not be applied. Including all security requirements in the contractual documents would clarify expectations of security to both RCMP staff and the vendor.

It is recommended that DSB and PMAM, in consultation with other government departments as required, should:

a) develop internal guidance and/or controls to ensure that RCMP security requirements are appropriately included in future contracts/SOs; and,

b) implement mitigating controls, where required, to address gaps related to RCMP requirements in the SRCL, recognizing that the SRCL is a central agency form not within the RCMP's span of control.

3.3 ADDITIONAL EXTERNAL SECURITY PROCESSES

Additional security processes for procurement may be applied under certain circumstances. Enhanced guidance is required on when to request additional security processes, such as FOCI, SCI and NSE.

The review identified several additional security processes and controls available for use when a procurement requires them, but the procurement of RF filtration equipment did not meet the requirements for their application. Examples of these additional security processes and controls include the Foreign Ownership, Control or Influence (FOCI) evaluation, Supply Chain Integrity (SCI) assessment, National Security Exception (NSE), Designated Organizational Screening (DOS) or Facility Security Clearance (FSC), and **********. Appendix B provides additional information on these processes and controls. Although the RCMP may provide input into some of these security processes, other government departments are primarily responsible for executing them.

While specific criteria exist to initiate a FOCI, SCI or NSE, none of these processes were triggered by the requirements for the Sinclair SO. It was noted that they can also be requested on a case-by-case basis through consultations between RCMP procurement and security officials and their counterparts in the government departments that manage these processes. These additional security processes may have significant operational impacts because they can prolong procurement processes. Although the RCMP has applied the use of FOCI, SCI and NSE in the past, the review found that the RCMP does not have formal guidance in its policy manuals on when additional security processes should be requested for procurements that do not meet the established criteria. The RCMP does not contribute to or have any authorities or responsibilities related to the DOS and **********.

It is recommended that DSB and PMAM, in consultation with other government departments as required, develop or enhance internal guidance related to additional security processes and controls, such as FOCI, SCI and NSE, and define conditions for when they should be requested as part of RCMP procurements.

4 CONCLUSION

The RCMP complied with applicable policies and procedures to establish the Sinclair Technologies SO for RF filtration equipment. Although subject matter experts confirmed that the equipment in this SO does not compromise secure communications based on the RCMP's application, some lessons learned and opportunities for improvement exist to enhance the consideration and articulation of security requirements in procurement processes going forward. Specifically:

- While it is important that requirements specific to the SO are understood by users to ensure that Call-ups are compliant with its terms and conditions, no recommendations were warranted in the context of this review.
- Guidance and/or controls should be developed to ensure that RCMP security requirements are appropriately included in future contracts/SOs, to ensure adherence by users. Gaps related to RCMP requirements in the SRCL should be addressed and mitigating controls should be implemented until the SRCL is modernized by central agencies.
- Guidance should be developed for additional security processes and controls such as FOCI, SCI and NSE and conditions defined for when they should be requested as part of RCMP procurements.

5 RECOMMENDATIONS

Policies and processes related to government procurement and security are owned by a variety of departments outside the span of control of the RCMP. As such, broader government engagement to modernize existing legislation, policies and tools is required to address future procurements that may have national security implications. In the interim, the RCMP can mitigate the risk through internal measures on an interim basis, specifically:

1.	**DSB and PMAM should, in consultation with other government departments as required:** **a) develop internal guidance and/or controls to ensure that RCMP security requirements are appropriately included in future contracts/SOs; and,** **b) implement mitigating controls, where required, to address gaps related to RCMP requirements in the SRCL, recognizing that the SRCL is a central agency form not within the RCMP's span of control.**
2.	**DSB and PMAM should, in consultation with other government departments as required, develop or enhance internal guidance related to additional security processes and controls, such as FOCI, SCI and NSE, and define conditions for when they should be requested as part of RCMP procurements.**

APPENDIX A – DESCRIPTION OF RADIO FREQUENCY FILTRATION EQUIPMENT[8]

All radios create, and are susceptible to, radio frequency interference. At radio sites, RF filters stand between antennas on the tower and two-way radios in the shelter, rejecting interference from nearby transmitters and passing only the correct frequencies to RCMP radios. Most RF filters are unpowered assemblies of tin cans, metal rods, magnetic ferrite blocks and coaxial cables. Some incorporate transistor-based amplifiers to boost faint incoming signals. The rods allow the cans to be tuned to precise frequencies and are used in equipment such as broadcast radio, wireless communications, and television. This equipment is used to optimize radio system performance and reduce impact on nearby services like cellphone, pager and satellite operations. Once installed and tuned, they typically remain in place for decades.

RF filters exchange no data with other equipment and are used to filter out unwanted signals. RF filtration equipment does not have the capability to access RCMP radio communications and poses no security concerns.

RF filters have several benefits.

• Permits RCMP radio receivers to receive communications more clearly by blocking interference and background noise, which is vital for making out faint or distant calls from officers and especially in emergency situations.

• Allows for several radio channels to use the same antenna, which supports concurrent police operations.

• Prevents RCMP radios from emitting RF interference that degrades the operation of other radio users at the tower site.

Radio antennas are passive devices used for only two purposes: 1) To send radio signals from transmitter radios to field personnel; and, 2) To capture radio signals and send the signal down a wire to receiver radios.

An antenna is considered passive as it only transmits the input signal received to other devices. RF antennas do not pose any security concerns with regard to access to data or voice information as they simply redirect energy. They are installed on towers and rooftops where they often remain for decades with little maintenance required beyond periodic inspection to ensure bolts are tight and cables are sealed.

[8] Source: Description provided by RCMP Specialized Policing Services

APPENDIX B – ADDITIONAL SECURITY PROCESSES

Foreign Ownership, Control or Influence

As part of its suite of security and oversight programs, PSPC can provide government programs with Foreign Ownership, Control and Influence (FOCI) evaluations. A FOCI assesses the degree of authority, ownership, control or influence that foreign interests may have over a Canadian organization. FOCIs can be requested by a program area when it is triggered as part of its policy process, as a result of a procurement clause, or through application of regulatory or legislated requirements. FOCIs inherently require a policy, contractual, regulatory or legislative foundation as they are a participatory process where a third party must either be encouraged, through the prospect of future economic gain, or compelled, by statute, to participate in order for the evaluation to be fulsomely carried out.

When leveraged in the context of PSPC's Contract Security Program (CSP), FOCIs help determine and mitigate the risk that unauthorized parties may exert undue influence over a Canadian organization to access government classified information and assets.[9] For purposes of administration of the CSP, PSPC is the owner of the FOCI process; the RCMP cannot conduct its own FOCI even if it was the contracting authority in a procurement process. The trigger for a FOCI evaluation is when an entity requires access to foreign classified/NATO/COMSEC systems, information or communications. The procurement of RF filtration equipment did not meet the requirements for a FOCI nor would have a FOCI assessment been the appropriate control measure to thwart supply chain vulnerabilities with the equipment.

Supply Chain Integrity

SCI assessments can be performed on Information and Communication Technology products and services that will be deployed onto Government of Canada infrastructure. SCIs safeguard the confidentiality, integrity and availability of the Government of Canada's communications and data by fostering resilience against digital supply chain vulnerabilities and compromise.[10] The Canadian Centre for Cyber Security is the owner of the SCI process. SCIs are product-specific and triggered on a case-by-case basis. The procurement of RF filtration equipment did not meet the requirements for a SCI.

National Security Exception

NSEs may be invoked to allow Canada to exclude a procurement process from some or all of the obligations of relevant international trade agreements to protect its national security interests.[11] At the RCMP, the requirement to invoke an NSE is typically raised by the Technical Authority, and PMAM and DSB are consulted. A request to invoke an NSE would be sent to PSPC if there is a clear case for one. The request is processed and approved by PSPC. The procurement of RF filtration equipment did not meet the requirements for an NSE.

[9] https://www.tpsgc-pwgsc.gc.ca/esc-src/msc-csm/chap3-eng.html#s33
[10] https://cyber.gc.ca/en/guidance/cyber-supply-chain-approach-assessing-risk-itsap10070
[11] https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/section/3/105

Designated Organizational Screening

DOS is a corporate level clearance designed to assess the reliability of organizations that have a requirement to access Protected A or B information or assets. Deliverance of a DOS allows an organization to request personnel security screening for their employees/embedded contractors at the Reliability Status level or in exceptional circumstances to obtain site access status.[12] PSPC is the owner of the DOS security assessment and the RCMP does not have any authorities or responsibilities related to this process. **********, the company was awarded the 2021 SO for RF filtration equipment because there were no security requirements associated with the SO nor the call-up that would have triggered a verification of the security status of the firm by the contract authority prior to awarding the call-up to the company.

****

[12] https://www.tpsgc-pwgsc.gc.ca/esc-src/organisation-organization/information-eng.html

APPENDIX C – MANAGEMENT ACTION PLAN

Recommendations and Management Action Plan

Policies and processes related to government procurement and security are owned by a variety of departments outside the span of control of the RCMP. As such, broader government engagement to modernize existing legislation, policies and tools is required to address future procurements that may have national security implications. In the interim, the RCMP can mitigate the risk through internal measures, specifically:

Recommendations	Management Action Plan
1. DS and PMAM should, in consultation with other government departments as required: a) develop internal guidance and/or controls to ensure that RCMP security requirements are appropriately included in future contracts/SOs; and, b) implement mitigating controls, where required, to address gaps related to RCMP requirements in the SRCL, recognizing that the SRCL is a central agency form not within the RCMP's span of control.	1. Agree. DS has increased the level of scrutiny on contracts to ensure appropriate controls are in place, pending more formal processes and policy direction as identified below. a) In collaboration with PMAM, DS will launch a pilot to review procurement requirements of sensitive law enforcement equipment/technologies that currently do not require an SRCL (i.e. when goods/services are not considered classified). The results of the pilot will allow the RCMP to review risks and processes and provide an opportunity to develop focussed guidance documents and/or necessary controls to ensure security requirements are appropriately addressed in future procurement activities more systematically. b) Referencing the results of the aforementioned pilot, DS, in consultation with PMAM, will develop and implement additional controls and guidance, as required, to address gaps in the existing SRCL form. Completion date: (a) The pilot is expected to be completed in summer 2023. (b) The review and assessment of results, as well as development of guidance documents and enhanced controls, will be completed by December 2023. Positions responsible: Chief Security Officer and Director General, Procurement, Materiel and Assets Management.

2. DS and PMAM should, in consultation with other government departments as required, develop or enhance internal guidance related to additional security processes and controls, such as FOCI, SCI and NSE, and define conditions for when they should be requested as part of RCMP procurements.	2. Agree, with a recognition of the RCMP's limited ability to lead change in this area. Notwithstanding, the RCMP is eager to support enhancements to security controls within government procurement. The RCMP will engage other government departments to collaborate on enhanced security processes within government procurement activities. Preliminary discussions in support of these recommendations have begun with TBS, Public Safety, and PSPC. Other partners in the Security and Intelligence community across the Government of Canada were also engaged to explore possible solutions, best practices, and lessons learned. With this information gathered, the RCMP will host two meetings: one with PSPC to share results of the review and to offer input as a client department. Second, the RCMP will meet with TBS to share shortcomings identified in the review, and offer input on possible enhancements to the SRCL. RCMP Senior Executives are also discussing security processes and controls related to the procurement of sensitive law enforcement equipment and technologies at Government of Canada engagement forums, including at the Public Service Management Advisory Committee (PSMAC). Based on the results of these meetings and the pilot project (Recommendation 1), DS and PMAM will develop specific guidance for RCMP programs on additional security processes and controls. The documentation will identify when FOCI, SCI, and/or NSE are required, and will clearly identify the steps that are required throughout the procurement process. Completion date: (a) Meetings with government departments and engagement with senior management forums to be completed by September 2023. (b) Guidance for RCMP programs to be developed by December 2023. Positions responsible: Chief Security Officer and Director General, Procurement, Materiel and Assets Management.