RCMP·GRC

ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

FEDERAL POLICING: FOREIGN ACTOR INTERFERENCE (FAI) STRATEGY

Protected B

May 26, 2023

Royal Canadian Mounted Police	Gendarmerie royale du Canada	Security Classification/Designation Classification/désignation sécuritaire **Protected B//For Internal**	Total Pages 22

Table of Contents

[APG]

Royal Canadian Mounted Police / Gendarmerie royale du Canada	Security Classification/Designation Classification/désignation sécuritaire **Protected B//For Internal**	Total Pages 22

Introduction

Foreign Actor Interference (FAI) is a dynamic and complex threat that includes any effort by a foreign state, or its proxies, to undermine Canada's national interests and values, or threaten public safety and the exercise of fundamental democratic rights and freedoms. FAI does not include legal and legitimate influence activities (such as cultural engagement or diplomatic activities); instead, it includes actions that are short of armed conflict, yet deceptive, threatening, and corrupt in nature. FAI includes a range of overt and covert threat activities, some of which are illegal and others which reside in a criminal grey zone between legal and illegal practices.[1] Foreign actors use these activities to advance their strategic interests, including: seeking geopolitical influence, domestic stability, and/or economic advancement; revising the rules-based international order; expanding authoritarian power at the transnational scale; and gaining certain military, health, scientific and strategic advantages. The RCMP is aware of FAI being perpetrated by different states, including (but not limited to) the People's Republic of China (PRC), Russian Federation (RF), and Islamic Republic of Iran. FAI can be strategically covert and overt. For instance, hostile state actors may leverage proxies (including serious and organized criminal groups or cybercriminals) to conduct FAI and this can make state attribution difficult. The RCMP is also aware of harassment and intimidation that is overt and targets communities, political dissidents, and human rights defenders, with the intention of exerting a hostile state's transnational power and influence in Canada. This indicates that both state and non-state entities conduct FAI-related activities.[2]

The evolving FAI threat is a central concern for the RCMP, Security and Intelligence (S&I) partners, civil society organizations, public institutions, the private sector (including businesses and corporations), and the Government of Canada (GoC). As the National Security and Intelligence Committee of Parliamentarians (NSICOP) wrote in their 2020 Annual Report, "Though the effects of espionage and foreign interference are not as readily apparent as those of terrorism, they are the most significant long-term threats to Canada's sovereignty and prosperity."[3]

The RCMP plays a significant role in responding to, investigating, and countering FAI. Pursuant to the *Royal Canadian Mounted Police Act*, it is the duty of RCMP officers to preserve the peace and prevent crime.[4] Subsection 6(1) of the *Security Offences Act* further designates the RCMP as the primary enforcement body in relation to threats to the security of Canada, as defined in Section 2 of the

---

[1] Grey-zone activities can be difficult to disrupt using law enforcement (LE) tools. For example, threats to research and technology may involve legal activities (e.g. procuring protected and proprietary information through talent programs) that are nonetheless detrimental to Canadian interests.

[2] CSIS Public Report 2020: https://www.canada.ca/en/security-intelligence-service/corporate/publications/2020-public-report/the-threat-environment.html#toc1

[3] National Security and Intelligence Committee of Parliamentarians Annual Report 2020: https://www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/intro-en.html

[4] Paragraph 18(a) of the RCMP Act notes it is the duty of RCMP members "to perform all duties that are assigned to peace officers in relation to the preservation of the peace, the prevention of crime and of offences against the laws of Canada and the laws in force in any province in which they may be employed, and the apprehension of criminals and offenders and others who may be lawfully taken into custody."

[APG]

Royal Canadian Mounted Police	Gendarmerie royale du Canada	Security Classification/Designation Classification/désignation sécuritaire **Protected B//For Internal**	Total Pages 22

Canadian Security Intelligence Service Act (CSIS Act), which includes acts of foreign interference (FI).[5] The RCMP may leverage any legislation or statute to counter FAI. Furthermore, the RCMP's *Operational Manual* describes the processes and procedures that RCMP officers adhere to, which ensure that investigations comply with judicial and court standards.[6] The RCMP is aware of sensitivities relating to counter-FAI investigations and balances the need for police independence with the understanding that police actions to counter FAI threat activities may have national and international political consequences. FAI, including the RCMP's criminal investigations of FAI activities, are both a matter of public interest and public safety.

Under its mandate, the RCMP investigates and works towards disrupting, and where possible laying criminal charges against, suspected foreign interference actors who may either be representatives of foreign states (e.g. intelligence agents), or proxies (e.g. individuals or groups of people that work at the behest or in the interest of a foreign state). The RCMP investigates suspected threat and criminal actors whom act on behalf of a foreign state; it does not investigate the state itself. The RCMP is aligned with the Government of Canada (GoC) in listing FAI as a priority in the RCMP's *Federal Policing 2020-2023 Strategic Plan*.

FAI poses a cross-cutting threat to Canada's national security, prosperity, and sovereignty, which means that FAI-related threats and illegal activities touch on all Federal Policing (FP) program areas. This demonstrates both the complexity of the issue, as well as the importance of working collaboratively. Collaboration is intrinsic to counter-FAI efforts and entails both internal collaboration between business lines within the RCMP, as well as the RCMP's ongoing collaboration with external partners, including other domestic and international Law Enforcement (LE), S&I, and Government departments. Currently, FP has four program areas in place to respond to the FAI threat:

1) Federal Policing National Security (FPNS), which provides oversight and support to Divisions conducting national security criminal investigations. FPNS program areas focusing on FAI include:
    a. Foreign Actor Interference Team (FAIT), which reviews, coordinates, and advises on matters of National Security related to illegal activities conducted at the direction or for the benefit of a foreign state, entity, and/or power. This includes providing governance on all FAI investigations across Canada undertaken by the Integrated National Security Enforcement Teams (INSETs) and National Security Enforcement Sections (NSESs);
    b. National Security Operational Analysis (NSOA), which provides Federal Policing National Security (FPNS) senior management and Divisions with a national and international operating picture relating to national security (NS) threats and investigations. This

[5] Paragraph 2(b) of the CSIS Act includes in its definition of threats to the security of Canada "foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person."
[6] See Operational Manual Chapter 20, including: Disclosure (ch.20.1) and Judicial Processes (ch.20.6).

[APG]

includes operational and tactical intelligence and analysis relating to FAI threats and investigations; and,

c. National Critical Infrastructure Team (NCIT), which captures intelligence and assesses physical and cybercriminal threats to critical infrastructure (CI) in support of the RCMP's and the Government of Canada's CI protection mandates, including FAI threats.

2) FP National Intelligence (FPNI), which, amongst other FAI-related responsibilities, participates in the Security and Intelligence Threats to Elections (SITE) Task Force, produces strategic intelligence products that inform senior management and GoC partners of FAI-related threat activity, and leads RCMP involvement in the national security review of foreign investments pursuant to the *Investment Canada Act* via the Economic Integrity Unit (EIU) team.

3) FP Criminal Operations (FPCO) conducts investigations that primarily target three areas with a nexus to FAI: cybercrime, serious and organized crime, and financial crime:
   a. FPCO Cybercrime targets the most significant cybercriminal threats to Canada's political, economic, social, and reputational integrity. FPCO-Cybercrime conducts investigations to identify and target cybercrime as a service, criminal networks conducting illicit activity in the cyber realm, and cybercrime events involving hostile foreign actors (state and non-state);
   b. FPCO Serious and Organized Crime (SOC) focuses its activities on associations of individuals whose goal is to obtain power, influence and monetary gain through corruption, violence and/or illicit schemes.[7] FPCO-SOC also investigates counter proliferation-related activities further to the *Special Economic Measures Act*; and,
   c. FPCO Financial Crime delivers national strategic direction, development, oversight, and coordination of federal financial crime programs. The mandate includes several areas where FAI could be detected and investigated from a criminal perspective, including Money Laundering (ML), Proceeds of Crime (POC) and Corruption, both foreign and domestic.

4) FP Sensitive and International Investigations (SII), which investigates threats to government institutions, public officials, the integrity of the Crown, or threats that otherwise imperil Canada's political, economic and social integrity.

While efforts to develop whole-of-government coordination and governance mechanisms to counter Foreign Interference (FI) are in development, a formal Strategy to counter FAI-related activity does not

[7] SOC encompasses a wide range of transnational illicit activities, such as: precursor chemical and drug trafficking, Encrypted Criminal Communications (ECC)/Hardened Secure Communications (HSC), illegal gambling, manufacture and trade in counterfeit goods, wildlife and cultural property smuggling, migrant smuggling, human trafficking, money laundering, black market firearms trafficking, fraud, theft, and extortion, which typically exploit provincial and national boundaries in order to execute their operations throughout Canada and abroad.

[APG]

currently exist within either FP or the GoC.[8] This FP-focused FAI Strategy, which was developed by FP Strategic Policy-National Security (FPSP-NS), provides an important step towards addressing this gap. It defines threats, outlines the actions FP is already undertaking to counter FAI (including identifying best practices), and lists future initiatives that will strengthen FP's ability to identify and respond to FAI. It outlines priority focuses to guide the future of FP's counter-FAI response (e.g. training needs, information sharing) and identifies opportunities and initiatives to leverage broader GoC efforts to strengthen the RCMP's approach to responding to FAI (e.g. legislative and regulatory updates, new policy directions, new funding requests). It has two core objectives: First, provide a way forward for FP on matters of coordination, public awareness, and training, and second, guide FP's involvement in future efforts by GoC partners – including Public Safety Canada (PS) – to develop a strategic, whole of Government response to countering FAI.

A Note on the Operational Campaign

Since May 2022, FPNS has been directing a national FAI operational campaign, which is independent of, but complementary to, the FP FAI Strategy. The Campaign's guiding vision is to lead the RCMP in strengthening Canada's response to FAI threats through robust assessment, collaboration, and disruption. Its mission is as follows:

- **Assess**: through collaboration, understand and prioritize FAI threat vectors and actors;
- **Advise**: inform internal and external stakeholders, promote awareness of FAI threats, engage victims; and,
- **Act:** through operational action, defend against FAI threats, disrupt, mitigate, or deter foreign threat actors.

It bears noting that the operational campaign is not focused solely on criminal charges but also on meaningful disruptions, impact, and mitigation of harm to Canada. Overseen by FPNS and working with other FP operational and intelligence sections, the Campaign assesses the threat picture and identifies opportunities for operational impact. It also provides the opportunity to enhance coordination on a counter-FAI response within the FP program.

To do this, FPNS leverages Working Groups focusing on particular operational priorities (e.g. technical operations, analysis and intelligence, and operational response) to advance the Campaign. These groups are comprised of internal and external stakeholders, including: implicated RCMP business lines, police of jurisdiction (POJs), domestic S&I partners (e.g. Canadian Security Intelligence Service [CSIS]

[8] In 2022, FPNS instigated an Operational Campaign to ensure a coordinated FP operational response to counter illegal FAI. More information on this is found below. s. 39 - Cabinet Confidence
s. 39 - Cabinet Confidence
s. 39 - Cabinet Confidence . As of Spring 2023, efforts to release a GoC counter-FI Strategy are still in development.

[APG]

and Public Prosecution Service of Canada [PPSC]), prevention and engagement units, and international LE partners. Strengthened collaboration with stakeholders ensures that the RCMP is not only continuing to maximize opportunities for enforcement action, but also maintaining awareness of counter-FAI efforts being effected by partners with nexus to Canada. By coordinating with partners to identify threats and determine the best way forward, the RCMP is strengthening its prioritization of efforts and maximizing the impact of its operations. NHQ will continue to provide governance and policy guidance to enable Divisions to identify law enforcement opportunities, prioritize investigative efforts, and achieve operational successes against FAI threats with the goal of achieving results.

An Action Plan complements this Strategy, and sets out a plan to implement the Way Forward Items articulated below. It bears noting that, as they develop, FAI-related efforts already underway within the RCMP will be leveraged to implement these recommendations (and related action items).

Strategy Methodology

FPSP-NS, in collaboration with FPNS, met with investigators and analysts from the following Divisions: B, C, D, E, F, G, J, K, L, and O (including Ottawa INSET). They also met with two units that were formerly housed in National Division (SII and Cybercrime), but are now in FP. Consultations included discussions with Divisional INSETs and National Security Enforcement Sections (NSESs). Discussions were held virtually through the MS Teams platform and conducted at the Protected B level for most Divisions, as well as at the classified level through a secured call at NHQ. Interviews were also held with various areas within RCMP NHQ that are responsible for reviewing investigative files, providing operational support, engaging public, private, and LE stakeholders, and conducting intelligence gathering functions related to FAI; these areas included: FPNI (including the EIU and Strategic Intelligence Analysis teams); FPCO, FPNS (including Operational Analysis and NCIT), FP Strategic Engagement and Awareness (FP-SEA), International, and the IE2 Team. The purpose of these interviews was to gather candid feedback on FP's current response to FAI, assess the organization's level of knowledge on FAI, and identify best practices, gaps and challenges encountered during investigations and intelligence work.

FAI Threat Examples

FAI poses an acute and cross-cutting threat to Canada's economy, national security, and public safety. Notable examples of FAI that have been the subject of public reporting include the following:

- in November 2022 the RCMP arrested and charged Yuesheng Wang, whom allegedly obtained trade secrets to benefit the PRC, to the detriment of Canada's economic interests, while employed by Hydro-Québec;[9]
- in Fall 2022 the RCMP began investigating reports of criminal activity relating to "police service stations" that are allegedly operating in Canada on behalf of the PRC;[10]

[9] RCMP News Release, Hydro-Québec employee charged with espionage: https://www.rcmp-grc.gc.ca/en/news/2022/hydro-quebec-employee-charged-espionage

[10] RCMP Statement, Reports of criminal activity in relation to foreign "police" stations in Canada: https://www.rcmp-grc.gc.ca/en/news/2022/reports-criminal-activity-relation-foreign-police-stations-canada

[APG]

- it has been alleged that foreign governments interfered in Canada's 2019 and 2021 federal elections, which has prompted the Prime Minister to announce several GoC measures to combat foreign interference;[11] and,
- there have been reports of Canadian citizens and residents being harassed, intimidated, and illegally surveilled by individuals aligned with the PRC[12] and Iran.[13]

FAI activities include, but are not limited to:

- **Threats to critical infrastructure**: state-backed physical and cybercriminal attacks on critical infrastructure systems, with the aim of illegally acquiring data, sabotaging system operations, or introducing vulnerabilities in key sectors;
- **Threats to democracy**: state-backed criminal interference in Canada's democratic institutions and/or elections systems, and influence activities that target politicians at all levels of government (i.e. municipal, provincial, and federal) and Canadian citizens (e.g. state-backed disinformation campaigns and AI-created Deep Fake audio and video recordings intended to disrupt elections);
- **Threats, Intimidation and Harassment of communities:** physical and cybercriminal violence and harassment, intimidation, and surveillance of communities, including political dissidents and family members located within Canada and abroad. Activities can include state-backed targeted assassinations and illegal renditions;
- **Threats to information/intelligence:** state-backed efforts to illegally acquire classified and protected government information, or theft of intellectual property (IP)/trade secrets through methods like espionage, insider threats, cyberattacks (including ransomware, advanced persistent threats, or developing and distributing malware), and other forms of tradecraft; and,
- **Economic threats**: the loss of sensitive technology, research, data, and IP; the malicious and criminal exfiltration and use of sensitive personal information of Canadians; market manipulation, illicit financing and money laundering (including financial network operators that facilitate the laundering and monetization of proceeds from cybercrime); investment in key Canadian resourcing industries; import, export, and proliferation of controlled and dual-use goods, goods with a nuclear nexus, and weapons of mass destruction; and targeted detrimental foreign investments in the Canadian economy under the *Investment Canada Act*.

---

[11] Prime Minster of Canada, Taking further action on foreign interference and strengthening confidence in our democracy: https://pm.gc.ca/en/news/news-releases/2023/03/06/taking-further-action-foreign-interference-and-strengthening

[12] House of Commons Special Committee on Canada-China Relations, Evidence May 31, 2021, Number 027, Notices of Meeting: https://www.ourcommons.ca/DocumentViewer/en/43-2/CACN/meeting-27/evidence.

[13] Human Rights Watch, May 27 2021: https://www.hrw.org/news/2021/05/27/iran-ukraine-airline-victims-families-harassed-abused# and Global Affairs Canada

[APG]

Priority Issues and the Way Forward

A. Training, Awareness & Operational Policy (High Priority)

While gaining subject matter expertise on FAI is a priority for personnel working on this file, opportunities to gain this expertise are available on more of an *ad hoc* basis. Consequently, operational personnel lack formalized awareness of the tactics and *modus operandi* leveraged by FAI actors, including an in-depth understanding of the variety of ways a foreign state conducts intelligence operations and procures protected and classified information from government and LE agencies. This is compounded by the lack of existing FAI policies and standardized operating procedures concerning FAI-related criminal activities that meet the NS threshold. This puts the RCMP at an operational disadvantage in countering FAI threat actors.

Consequently, consultations with RCMP FAI stakeholders revealed that there is a strong appetite for FAI-related training for FP personnel, RCMP Divisions, and POJs working in the national security space.

Inconsistent investigative practices are being used across the Divisions, which has resulted in *ad hoc* approaches to conducting FAI investigations. This approach is further exacerbated by the lack of FAI-specific policy and standardized operating procedures.

Efforts to address these gaps are underway. For instance, an introductory FAI module was added to the National Security Criminal Investigations (NSCI) course in November 2019 and a threat landscape component was added in 2022. However, apart from these mondules, stand-alone training that focuses on FAI is not currently available from the RCMP, which has resulted in knowledge gaps between Divisions with respect to FAI threats and indicators. There are keen and enthusiastic investigators conducting their own research to gain requisite familiarity with, and knowledge of, FAI. Despite this impressive dedication, the resources officers rely upon are not consistently vetted by subject matter experts for accuracy or quality. This produces gaps in the consistency, comprehensiveness, and specificity of FAI-related information available to, and accessible by, officers and investigators. In one example, a unit developed their own internal guide to support officers within that INSET working on these files. It provided advice on appropriate precautions to undertake (e.g. ensuring that documents are property classified, that secure communications are used, and providing advice on how to meet with victims that may be subject to state surveillance). Analysis is ongoing to determine whether this document could become a 'best practice' shared with other Divisions.

Stand-alone training and information resources focusing on pertinent FAI information, which are made available to all FAI-focused personnel would ensure consistency in both the quality of FAI-related information, as well as the ability for personnel to access that information.

The Way Forward (High Priority)

[APG]

Royal Canadian Mounted Police / Gendarmerie royale du Canada	Security Classification/Designation Classification/désignation sécuritaire **Protected B//For Internal**	Total Pages 22

1. ***Develop introductory/"FAI 101" Agora course (at Protected B level) that defines FAI, including: threat environment, threat indicators, security/classification issues relating to information handling, procedures for secure information exchanges with international LE and S&I partners, and relevant legislation that can be leveraged by investigative units to counter FAI activities (including Security of Information Act (SOIA) and relevant Criminal Code offences). It should target a large audience and be shared with RCMP personnel across business lines, including: POJs, Divisions, and NHQ. As it will be circulated via Agora, threat-related information will be introductory and primarily unclassified.***

   NOTE: Opportunities to share this training with police services outside the RCMP (including larger provincial and municipal agencies) should be explored to ensure coordinated understanding of FAI-related threats, concerns, and threat indicators. Opportunities to include the PPSC in the development of this training and offer it to other stakeholders should also be explored to develop coordinated understanding of FAI-related legislation and Criminal Code charges. Efforts are underway to identify opportunities to provide webinars and guest lectures from academic and subject matter experts on FAI-related topics – offered at the unclassified level. Presentations from the Academic Outreach program at CSIS could be leveraged when relevant items are presented. Domestic and FVEY S&I and LE partners could also be engaged to solicit content and best practices relevant to this training. GBA Plus and cultural awareness considerations will need to be addressed in, and built into, the development of training materials.

2. ***Develop specialized and comprehensive training that covers FAI-related investigative considerations, including: threat landscape, disruption and investigative concerns and techniques, counter-surveillance matters, use, storage, and/or disclosure of classified information related to counter-FAI investigations. Due to the sensitivities relating to FAI criminal investigations and threats, the training will need to be developed and offered to investigators at the classified level.***

   NOTE: The Canadian S&I community and Five Eyes (FVEY) partners could be engaged for best practices in the development of this training material. Opportunities to leverage existing training materials and information resources could also be explored. Guest lectures provided by specialists, experts, and/or RCMP investigators with enhanced and/or applied experience in FAI investigations could also provide an immediate and low-cost approach to bolstering training materials and enhancing FP awareness of both the FAI-related criminal activities targeting Canada, as well as the appropriate and effective investigative techniques with which to counter these activities. GBA+ and cultural awareness considerations will need to be addressed in, and built into, the development of training materials.

[APG]

Royal Canadian Mounted Police / Gendarmerie royale du Canada	Security Classification/Designation Classification/désignation sécuritaire **Protected B//For Internal**	Total Pages 22

3. ***Develop operational policy specific to FAI, to provide further guidance to frontline personnel on considerations including: NS threshold, Operational Security, secure handling of operational information, and the One Vision process.***[14]

   NOTE: Domestic and FVEY S&I and LE partners could be engaged to solicit best practices and lessons learned as well as to learn from their own established policies. As well, aligning proposed and actioned operational policy updates with intelligence partners (e.g. CSIS) to ensure threshold, mandate and deconfliction are as clear as possible would be advantageous. Work is already underway to review and update Section 12 of the Operational Manual (OM), and any review of operational policy should account for, and align with, updates made to the OM.

B. Intelligence (High Priority)

RCMP criminal intelligence collection and analysis fulfills two broad objectives: 1) Producing a national operating picture to inform criminal investigations, and 2) Informing senior managements' decision-making on operational and strategic matters. These functions necessarily include FAI-related intelligence. However, RCMP intelligence collection is primarily responsive and investigations-led, rather than being proactively developed within NHQ, and attentive to NS mandate priorities. Furthermore, the RCMP is also reliant on external partners for FAI-related intelligence.

As such, in Divisions, there is inconsistent capacity to collect and analyze FAI-focused intelligence. Some Divisions are well-positioned and already developing their own intelligence and allocating intelligence analysts to focus on FAI; others lack the capacity, resources, and awareness of the threat environment to proactively develop intelligence. This impacts overall awareness of the extent of FAI threats and criminal activities across Divisions and FAI investigations. A fulsome capacity and needs assessment of FP's counter-FAI intelligence capabilities has not yet been undertaken.

Altogether, personnel in both NHQ and Divisions have inconsistent access to informative and actionable intelligence; this is further exacerbated by ongoing issues in translating "intelligence to evidence."[15]

The Way Forward (High Priority)

4. ***Continue engaging with intelligence agencies (e.g. CSE and CSIS) to determine the level of detail in information disclosed to the RCMP, which is required for FP to effectively take action against FAI.***

   Note: Current work related to intelligence to evidence processes being undertaken by the RCMP's IE2 team will be an ongoing consideration for this recommendation. Similarly, efforts to inform

[14] A manual on disruption considerations is under development. This type of operational policy will be beneficial for personnel working on FAI files.

[15] Divisions will not be able to obtain certain intelligence-related information due to caveats – this will continue to occur on a case by case basis.

[APG]

policing personnel on the potential uses of "non-actionable" intelligence and information provided by intelligence agencies in a policing context should be continued and awareness of how to use this information should be increased within the RCMP. For example, information can be leveraged to develop investigative leads, as grounds in a judicial authorization, or as evidence in a criminal prosecution.

5. ***Survey the RCMP's intelligence capacity and capabilities to assess organizational requirements to effectively counter FAI threats at the national level. RCMP-developed intelligence will provide a strong starting point to address broader "intelligence enabling evidence" issues that were also flagged in consultations with both Divisions and NHQ.***

   NOTE: FP should explore coordinating and centralizing information and intelligence-sharing through NHQ (further the need to know/right to know principles), ensuring that relevant intelligence received from Divisions is then re-shared across Divisions. To ensure this is done in a secure manner, this could be achieved by adding analytical resources to an appropriate unit or team that is identified, to take on this activity, if required. As well, FPNS could draft operational intelligence products with Divisional information included that provides a national operating picture of FAI-related investigations, the threat environment, and other operationally relevant pieces. Should there be a need for additional resources to take on this work, a business case could be developed in support of an associated funding request.

6. ***Further leverage intelligence-gathering efforts transpiring within other RCMP areas – such as International Liaison Officers and Analysts Deployed Overseas embedded in numerous areas around the world and informants linked to FPCO investigations – as a means to strengthen FAI-related intelligence and investigational leads.***

C. Legislation (High Priority)

INSETs and NSESs experience difficulties with investigating and laying charges under *SOIA*. Almost all Divisions described this legislation as difficult to work with, whether citing the lack of *SOIA* case law, or the need to be able to prove under *SOIA* that certain FAI-related activities actually benefit a foreign state. *Criminal Code* offences were described as the preferred mode of advancing criminal charges, but these charges lack "foreign state-backing" as a potential aggravating factor in sentencing. The RCMP, PPSC, and Provincial Crown should continue to work together to increase awareness and provide joint training to prosecutors and investigators about the challenges of investigating and prosecuting FAI cases. This includes the application of Section 38 of the *Canada Evidence Act* and the roles of the Attorney General and Federal Court in this process.

Because FAI threats are inconsistently captured in Canada's current legislation and regulations, there is a need to continuously review FAI-related legislative frameworks, policies and mechanisms from FVEY partners to determine areas where comparable approaches can be implemented within the Canadian context (e.g. Australia's 2018 NS legislation amendments, the United States' Foreign Agent Registry, or

[APG]

the United Kingdom's NS Bill). Related to the current policy practice of conducting its own research on FVEY FAI-related legislation and policies, FP is currently supporting ongoing activities within the GoC, analyzing such mechanisms, and contributing to the implementation of similar and relevant approaches in Canada. Specifically, FP is involved in and supporting GoC efforts to develop a Foreign Influence Transparency Registry, which would require individuals or entities acting on behalf of a foreign state to formally identify and register the purpose of their activities in Canada. In March 2023, public consultations on a registry began within Canada; similar legislation is already in place in both Australia and the US.[16] Opportunities to leverage the FAI-related work on amending legislation to bolster Canada's counter-FAI criminal offences to also address ongoing "intelligence to evidence" issues should also be explored.

Upgrading criminal legislation and enhancing general awareness of relevant and appropriate offences in FAI investigations across the RCMP, PPSC, and Provincial Crown will strengthen counter-FAI responses. However, the covert and clandestine methods used by hostile state actors in FAI also provides an opportunity to rethink criminal prosecutions as the "gold standard."[17] Collaborations with S&I partners should take place to develop and implement alternative and coordinated disruption measures – e.g. regulatory sanctions, financial intervention, and/or immigration inadmissibility – to counter FAI and uphold public safety by strategically leveraging and coordinating mandates. [18]

The Way Forward (High Priority)

7. ***Work with other government departments/agencies, particularly PS and the Department of Justice, to support the review and update of relevant legislation, including: SOIA, to provide for more applicable offences to target FAI, and the Criminal Code, to render a more acute and pronounced consideration of state-backing as a potential aggravating factor for otherwise routine offences.***

8. ***Review relevant FVEY legislative frameworks to identify legal avenues, best practices, and support development of similar policies and legislative efforts in Canada, including supporting current PS-led efforts to create a new foreign influence registry, in line with US/Australia models.***

   NOTE: As relevant Canadian and FVEY legislation is reviewed and updated, it will also be opportune to revisit how FP considers FAI threats to be successfully addressed, and whether the emphasis should remain on criminal prosecution. Given known challenges with SOIA and the Criminal Code, where criminal prosecution may not be possible, the RCMP could and should, for

[16] The Foreign Influence Transparency Scheme (FITS) and Foreign Agent Registration Act (FARA), respectively.
[17] Both the *Operational Improvement Review* (2018) and *One Vision 3.0* (2021) reflect that prosecution is no longer the gold standard: public safety is instead. The counter-FAI space offers opportunities to implement an existing FP commitment. Furthermore, attention could also be given to reviewing and identifying other relevant existing (but under-utilized) legislation that could be applicable to laying charges against criminal FAI.
[18] FPCO-Cyber leverages disruption methods to lawfully dismantle, seize, and/or shut down cybercrime infrastructure and assets used to harm and exploit Canadians – a similar focus on disruption methods would strengthen FP's counter-FAI posture and approach.

[APG]

example, leverage other Acts of Parliament, including the Immigration and Refugee Protection Act (in collaboration with the Canada Border Services Agency) or the Public Service Employment Act, among others, as appropriate, to counter FAI. As well, FP could also proactively engage GoC and S&I partners to strategically leverage mandates to safeguard Canada's interests.

D. Operational Resources (High Priority)

FPSP-NS maintains a regular dialogue with operational units and other program areas involved in FAI. It also monitors new and emerging GoC funding and policy mechanisms to identify and articulate proposals for new investments for the RCMP. Nonetheless, there are evident and urgent gaps in the resources available for the RCMP to counter FAI. Divisions face resource constraints, which impact their capacity to conduct both proactive and reactive FAI-related investigations. For instance, Divisions flagged both an unstable resourcing base to conduct investigations (including the need to second investigators from other program areas to conduct NS criminal investigations), as well as the need to stop and start investigations when newer, more urgent files come in. There is also a resourcing gap in NHQ units involved in FAI files, including the lack of analysts and reviewers in the FAI team in FPNS, FPNS' Operations Analysis team, and the EIU in FPNI. Recruitment and retention remain key issues that hinder the work of each unit, and the current FTE complement is not commensurate with the ever-increasing workload. Efforts to bolster resources should not only address current gaps, but also include the development and maintenance of a dedicated analytical cadre housed in FPNS for the development of usable intelligence for operational advantages.

Divisions also require appropriate infrastructure as they currently have inconsistent access to secure VTC and case management systems, thus producing gaps in access to secure communications and file management technologies. It is essential that discussions of FAI-related investigative and disruption techniques, and considerations, consistently transpire at the SECRET level. However, both Divisions and NHQ utilize ROSS for file management and storage purposes (up to the Protected B level). Both GoC and LE computer networks and information systems are targets of interest for FAI threat actors, whom are highly capable and determined to extract and procure sensitive and protected information. It is an ideal time to conduct a security review of these systems for potential vulnerabilities.

Additionally, FP does not currently have a robust and consistently distributed capacity to translate data in a foreign language that may be valuable for investigative purposes. Enhancing translation capacity – including both software and human personnel – in Divisions and NHQ should be explored due to the unique nature of FAI-related investigations, which often include reviewing large volumes of data that is in languages other than French or English. While St. Roch translation software was flagged as benefitting a cross-section of translation efforts within select Divisions and NHQ, consultations also revealed inconsistent access to, and awareness of, this software. Furthermore, personnel described struggling to translate the large volume of information with which they were dealing.

[APG]

The Way Forward (High Priority)

9. ***Conduct a review of technology available in Divisions to ensure they have appropriate access to required tools (CE, secure VTC, Tier 3 workstations, software, etc.), and outfit with systems needed where required.***[19]

10. ***Conduct a security review of communication channels/devices, computer networks (including the ROSS drive), and classification levels of personnel involved in FAI files to identify vulnerabilities.***

11. ***Develop and onboard personnel, specifically focusing on high-need areas (e.g. subject matter expertise, cyber skills, counter-surveillance, translation services, etc.).***

NOTE (WF Items 9-11): Budget 2023 proposes to provide $48.9 million over three years on a cash basis, starting in 2023-24, to the RCMP to protect Canadians from harassment and intimidation, increase its investigative capacity, and more proactively engage with communities at greater risk of being targeted. s. 39 - Cabinet Confidence ***business lines have been consulted to identify resource needs and gaps. It should be noted, however, that while Budget 2023 proposes $48.9 million for the RCMP to counter the above-noted foreign interference activities, this proposed funding, while necessary, is not commensurate to the threat, including for the countering of the various ways that foreign actors may leverage technologies to advance their objectives. As such, FPSP-NS will continue to seek additional mechanisms to secure funding to support the above resourcing requests. This includes identifying MCs, Treasury Board Submissions, or other appropriate instruments that may provide for the ability to obtain FAI-related resources when required.***

As well, to encourage accountability and implementation of requisite security measures, a yearly review of information-related computing infrastructure and security processes could be implemented, which may enable security measures to be adopted or adapted more regularly. The reviews would also highlight specific outcomes that can be achievable in the short and long term. Tech Ops support will also need to be considered for this initiative to upgrade operational resources, as enhancements to the FAI-related response will require appropriate Tech Ops support.

[19] Progress has been made on secure communications-related implementation. For example, E Division currently has secure communications capabilities, and K Division has the capability to have secure communications implemented, although construction would be expensive.

[APG]

Royal Canadian Mounted Police / Gendarmerie royale du Canada	Security Classification/Designation Classification/désignation sécuritaire **Protected B//For Internal**	Total Pages 22

E. Data Integrity & Collection (High Priority)

The RCMP has several Information Management and Information Technology (IM/IT) programs, which are focused on strengthening data governance, integrity and management. This includes FP Accountability and Oversight, which has a dedicated team of analysts in the Situational Awareness and Support Unit (SASU) that work with FP program areas to address gaps and develop best practices in data management for all of FP.

While there have been evident advancements in addressing broader data integrity across the Organization, in discussions with investigative teams it became clear that Divisions lack specific procedures, outside of recording in PROS/SPROS, to distinguish whether an investigation has an FAI component. Moreover, the process for recording file-related information in PROS/SPROS is not consistently clear – thus potentially impacting the amount of FAI-related investigations reported. These gaps could result in broader data integrity issues, such as an inaccurate number of the types of FAI investigations that may actually be occurring. As well, there is no process in place to track files that, for instance, may have started as an FAI investigation but were found to be non-FAI related and sent to POJs for furtherance. Further, the RCMP does not have a centralized location for FAI-related investigational information. Currently, RCMP INSETs and NSESs house their investigative information on several different databases including, MAPO, SPROS, E&R and PRIME. This is a broader issue that cross-cuts all NS files, including FAI files, that hinders the ease with which reviewers and analysts in NHQ can access and make connections regarding FAI information. This lack of centralized access to relevant information can have further downstream impacts on analytical products and decision making. As well, there is inconsistent information sharing between Divisions and NHQ analysts, thus further limiting NHQ analysts' access to relevant information. Addressing these issues in data integrity and access will help to clarify the scale of FP's involvement in FAI-related investigations and/or disruption efforts.

The Way Forward (High Priority)

12. ***Explore enhancing data integrity in recording FAI-related investigations within PROS/SPROS systems (e.g. developing a drop-down menu specifying threat vectors Critical Infrastructure, Harassment & Intimidation, Economic Security, Research Security) and suspected countries/states under investigation.***[20]

    NOTE: This will allow for improved awareness of the threat picture, as well as enable more data-informed consideration of alternative actions/disruption techniques that may be required for future FAI investigations (e.g. if there is an evident trend of investigations that were dropped due to certain evidentiary thresholds for prosecution, it could demonstrate the opportunity and/or need to shift to disruption techniques in certain instances/for certain types of investigations). As well, developing an approved methodology to identify suspected countries/states within SPROS/PROS will also help to enhance data integrity. However, data entry in PROS/SPROS is classified at Protected B; consequently, records/information security personnel will need to be

[20] Addressing data integrity issues will entail balancing a focus on individual files, analysis, and action.

[APG]

engaged to ensure information systems integrity and/or to determine an appropriate and efficient systems solution. Updated training in PROS/SPROS will be required, to ensure that these systems are being used appropriately.

As well, there is currently no means to capture gender data within the RCMP's records management system. Statistical analysis related gender data, if/when required, cannot be performed without the required fields and ensuing data.

F. Public Reporting and Awareness (Medium Priority)

FAI can target those that fear reporting to LE officials. This impedes FP's ability to attain and maintain visibility on FAI threat and criminal activities, as these activities are very likely underreported. This includes targeted communities, human rights defenders, or political dissidents that are not reporting instances of harassment and intimidation due to threats of physical harm or death (to either themselves or family members whom are still in a third country); witnesses/complainants that refrain from providing statements to investigators that could be detrimental to foreign entities/states for fear of reprisal; and certain public, private, and/or government entities and agencies refraining from reporting cybercriminal and ransomware attacks, or theft of IP, proprietary technology and research, for fear of reputational damage. FP-SEA develops and conducts outreach and engagement with POJs and First Responders to bolster their awareness of how to report NS-related threats and suspected illegal activities to the RCMP. They also develop presentations and information resources, which are provided to Divisions, to support and inform their engagement with communities on NS-related matters. The RCMP also provides information to the public, via its communications activities and website, on its National Security Information Network (NSIN), which provides members of the public the means to report suspected NS-related illegal activities. Efforts should continue to be made to ensure that this information is available and accessible, to ensure that the public is aware of how to report suspected FAI threats and criminal activities to LE. As these efforts continue and are strengthened, consideration will also need to be given to the safety and security of those reporting FAI-related activities, as well as impacted third parties (e.g. family members), as foreign states have significant reach and are highly resourced to be able to retaliate.

Ensuring these resources are disseminated widely and available to LE stakeholders and members of the public will continue to be an essential piece to countering FAI, as it will strengthen the RCMP's awareness of, and response to, the public's reporting of FAI criminal activities.

The Way Forward (Medium Priority)

13. Continue increasing the public's awareness of FAI and continue to inform the public on the recommended procedures to follow when reporting FAI-related concerns. This should include updating the RCMP's NS website to include more details about FAI (including adding FAI-related details under its "NS Awareness" and "Guide to Reporting Suspicious Incidents" webpages). As well, an online campaign that explains the steps the public should take to report the activity, and providing the relevant contact information (e.g. reiteration of 1-800 numbers, e-mail addresses

[APG]

such as the National Security Information Network e-mail, or any other contact information that should be provided) should also be produced and widely disseminated. As well, information should be provided on what will occur once the RCMP has been contacted. Efforts should continue to ensure that any new information materials are available in various foreign languages (e.g. Mandarin, Cantonese, Punjabi, Arabic, Persian, etc.) and be distributed to NHQ, POJs, and Divisions to ensure alignment of public messaging and RCMP awareness.[21]

NOTE: Protecting the safety and anonymity of individuals that report suspected FAI-related criminal activities should be considered as the public reporting process is further coordinated and upgraded. The public should be able to report suspected FAI-related threat and criminal activities without fear of reprisal, which means that they need to be able to do so with reasonable anonymity and protection. Establishing procedures for public reporting needs to be done in combination with development of FP-SEA materials and both need to be based in the relevant GBA+ / Cultural awareness analysis of the highest priority FAI target communities. Having reporting procedures that work well with existing RCMP reporting systems is not enough if they are not also designed to be trusted and easily useable by members of populations and communities targeted by hostile state, criminal, and/or threat actors.

G. Bolstering Coordination (Medium Priority)

While personnel in Divisions are largely familiar with whom to contact in case support on FAI-related investigations is required, there is strong interest in formalizing FAI-related partner engagement within FP. This is because partner engagement is undertaken in a more *ad hoc* manner across Divisions. Specifically, while some Divisions spoke to their regular engagement with contacts in other Divisions on FAI-related matters (thus demonstrating a good step towards operational collaboration between Divisions), others discussed their lack of familiarity with other FAI-relevant Divisional contacts. As well, there was inconsistent understanding, in Divisions, of FPNS' role in governing and facilitating engagement with other government and S&I agencies (both domestic and international).

Moreover, there are gaps in both information about, as well as knowledge of, FAI activities and initiatives within FP. This was raised in discussions held with both the Divisions and NHQ. There is a need for all implicated personnel (i.e. operational, intelligence, data analysis, communications, engagement, and policy) to develop more formalized means of information exchange to strengthen awareness and understanding of FAI-related issues. FP's response to FAI crosscuts business lines (from strategic intelligence products, to the creation of policy options; from briefing senior executives on decision-making, to conducting outreach and engagement with stakeholders) and there is an acute need to develop more consistent and formalized means of information exchange among FP FAI stakeholders. Doing so would ensure that activities (including research, investigations, and/or engagement efforts) are coordinated.

---

[21] PS-led initiatives relating to strategic communications and engagement s. 39 - Cabinet Confidence should be identified and leveraged to raise public awareness.

[APG]

As described above, under the Campaign, several working groups with an operations focus have been convened; furthermore, in response to the appointment of the Independent Special Rapporteur to conduct a study on alleged FAI targeting the 2019 and 2021 federal elections, an FAI Coordination Group has been stood up (comprised of intelligence, policy, operations, legal, and external review stakeholders). A similar structure could be leveraged to form a group focusing on strategic FAI issues (e.g. communications, policy, data integrity, engagement and awareness, and performance results reporting). Convening this WG, which would be comprised of internal RCMP partners (e.g. FP-SEA, FPSP-NS, FP Communications, FP-P&R, and FP-SASU), could foster common approaches, enable the sharing of relevant information, and improve organizational awareness of FAI-related strategic issues. It would increase efficiencies by encouraging internal collaboration on, and information sharing about, FAI-related matters within the RCMP. Divisions would then be informed of issues that arise at these WGs through the existing FPNS oversight and governance structure.

In Winter 2023, several recurring, inter-departmental and senior executive-level committees specifically focusing on countering Foreign Interference were stood up, including: FI meetings for Assistant Deputy Ministers (ADMs) and Deputy Ministers (DMs), and an ADM Transnational Repression committee. It will be important for these meetings to continue, as Strategy-related consultations indicated strong interest in convening an external Working Group comprised of other government and security partners (e.g. CSIS, CSE and Global Affairs Canada) to ensure a "whole of government" response to FAI. A formalized and regularly convened interdepartmental WG focused on FAI will enable: the timely sharing of information and intelligence, developing joint or collaborative analytical assessments, and operational collaboration. Opportunities to leverage existing forums (e.g. the Five Eyes Law Enforcement Group (FELEG) or Canadian Association of Chiefs of Police (CACP)) to facilitate more regular discussions of FAI with international partners should continue to be explored, as FAI impacts both Canada and its allies. Several Working Groups currently exist to facilitate FVEY discussion and collaboration with European partners (for instance at EUROPOL). The RCMP should evaluate which of these fora would be best for enabling international coordination, including the potential leveraging of INTERPOL to assist as well.

The Way Forward (Medium Priority)

14. Stand up an FAI working group that is internal to the RCMP and comprised of members that focus on strategic FAI-related issues in NHQ to: share best practices; identify gaps & challenges; communicate policy updates and intelligence products; and coordinate efforts to respond to FAI.

NOTE: This effort would consist of a FAI Working Group, comprised of NHQ areas involved in FAI-related matters (e.g. FPNI, FPNS, FPSP-NS, and FP-SEA). A structured and permanent internal RCMP FAI Working Group would enable opportunities to formally share, discuss, and strategize: FAI considerations in policy, operations and intelligence spheres, lessons learned, best practices, and threat awareness. Divisions would stay apprised of developments at this working group through the existing FPNS governance and oversight function.

[APG]

This WG would also provide opportunities to enhance coordination and collaboration between FAI-focused units in NHQ, strengthening the development and advancement of strategic issues and initiatives that support Operational responses to illegal FAI. To ensure alignment and deconfliction of efforts, it will be necessary to define clear rules of engagement, file triaging, and establish ownership of FAI activities within FP (further discussed in WF item 16).

15. ***FP should continue to participate in interdepartmental and interagency FAI-focused committees and WGs (e.g. ADM FI, DM FI, and ADM Transnational Repression). These WGs provide opportunities to discuss how the mandates of the various departments and agencies can be leveraged and strategically coordinated to counter FAI, deconflict efforts, and better coordinate information sharing.***

16. ***FPNS should continue to direct a national operational campaign that is separate from, but complementary to, the FAI Strategy. The national campaign will build off the policy foundation set by the Strategy and focus on enabling and advancing the RCMP's operational response to FAI across the Divisions, and in collaboration with both Government of Canada and external partners.***

    Note: The FPNS FAI team is currently leading the Campaign and plays a central and leading role in prioritizing, planning, and coordinating efforts and initiatives that will improve the operational response to FAI.

H. FAI Definitions (Medium Priority)

There is not yet a clear consensus across the GoC on a definition of FAI. While paragraph 2(b) of the *CSIS Act* is a significant piece of legislation that sets out the parameters of FAI, it is termed "foreign influenced" activity. It should also be noted that, until late Fall 2022/Winter 2023, both the GoC and PS favoured the term "hostile activities by state actors" (HASA) to describe the range of criminal and grey zone activities affiliated with foreign interference. The term used to describe HASA has now been changed to foreign interference (FI). FP primarily targets and counters FAI, which was treated as a sub-component of HASA, in that FAI focuses on the actor and/or group that has perpetrated HASA. Yet in the 2020-2023 FP Strategic Plan, Foreign Interference Activities is listed as a NS priority. Consultations with Divisions also indicated a lack of clear consensus on not only what entails FAI, but what term to use to describe this sort of threat activity. The lack of consensus, both within and across the GoC, FP, and the broader S&I community, further obfuscates general awareness and understanding of what is already a complex and grey-zone threat to Canada's national security and sovereignty. Furthermore, FAI entails a complex threat environment that does not adhere to any particular organizational silo, interweaving other areas (e.g. organized crime, border integrity, transportation, financial crime, and political corruption). Therefore, while FAI falls under FPNS's mandate, threats and criminal activity manifest in other RCMP areas, such as Border Integrity, SOC, and Sensitive Investigations. Consequently, FP may have multiple teams doing counter-FAI work that is duplicative and uncoordinated. Establishing clear definitions and jurisdiction for counter-FAI efforts will be integral to both define and strengthen RCMP response to this threat as well as broader inter-departmental awareness and understanding of the complexity of the threat and the RCMP's response.

[APG]

The Way Forward (Medium Priority)

17. Support and contribute to broader GoC and multilateral efforts to define terminology that will contribute to the development of a definition for FAI.

NOTE: FAI is the preferred term prioritized and articulated in FP. There are existing documents already on-hand (e.g. decks, briefing packages for senior management, and Strategy and Campaign documents) that articulate a working definition of what FAI entails, which is cross-referenced with CSIS Act 2(b). This definition should be leveraged for broader GoC efforts. Implementing this recommendation will include: (i) Updating operational policies and manuals to provide clear definitions of FAI-related terms (including actor, interference, and influence);[22] (ii) Establishing and clarifying jurisdiction for counter-FAI activities within the RCMP's program areas/business lines; and (iii) ensuring these terms align with those used in CSIS and CSE. While FAI falls under the mandate of RCMP's national security program, FAI poses a complex threat that interweaves several areas (including SII, FPCO, and SOC).

I. Engagement with POJs and Communities (Medium Priority)

Communities are often the targets of a foreign government's activities. While academic exchange programs can be leveraged as a means to extract data, research findings, and/or other proprietary and protected information, it is also important to note that FAI can also be exerted through domestic proxies. There is inconsistent understanding of when and how to conduct and deconflict outreach and engagement efforts. Some Divisions spoke of doing *ad hoc* outreach with certain academic, research, and commercial entities to raise awareness of FAI threats in those sectors. Others communicated either reluctance in pursuing, or lack of knowledge on how to perform, these sorts of activities. Raising awareness of FAI threats within impacted areas (whether commercial entities or critical infrastructure sites) in a coordinated manner that deconflicts with the outreach and engagement efforts of other government departments and S&I partners is a priority. Awareness of how outreach and engagement is happening, either across the RCMP, between POJs and Divisions in certain geographic regions, or within other S&I partners is inconsistent.

Divisions also expressed concern with the potential lack of cultural awareness and competencies to conduct outreach and engagement with the diaspora and ethnocultural communities targeted by state-backed harassment and intimidation campaigns and activities. This poses a potential impediment to a robust counter-FAI response, supported by community buy-in.

---

[22] As work is already underway to review and update Section 12 of the *Operational Manual* (OM), any review of operational policy should account for, and align with, updates made to the OM.

[APG]

Royal Canadian Mounted Police	Gendarmerie royale du Canada	Security Classification/Designation Classification/désignation sécuritaire **Protected B//For Internal**	Total Pages 22

The Way Forward (Low Priority)

18. Develop clear frameworks/guidelines to distribute to Divisions that provide guidance and support resources for officers and investigators conducting engagement and outreach activities with POJs and communities experiencing state-backed harassment and intimidation, as well as the private sector. Currently, this is done in an ad hoc manner, with minimal oversight and coordination.

NOTE: FP-SEA has several initiatives underway to bolster awareness of FAI threats and indicators with first responders and POJs, as well as with communites. Opportunities to leverage this work should be ongoing and prioritized.

J. GBA Plus Awareness and Policy (Low Priority)

FAI targets all members of the public, including Indigenous communities and other racialized Canadians. While efforts to better define FAI, both within RCMP operational policies and within broader legislation and GoC efforts, are much-needed, it will also be essential to conduct this work with a pronounced consideration of GBA Plus factors. There may be potential biases for analysts, reviewers, and investigators, embedded in Divisions and NHQ, to unpack and address in order to more effectively develop operational responses to these threats. Namely, while there are certain foreign governments backing, sponsoring, and/or supporting FAI targeting Canadian interests, those government activities are not synonymous with either the citizens of those countries or domestic diaspora and ethnocultural communities. A focused application of GBA Plus, bolstered by engaging GBA Plus focal points, will strengthen understanding of the targets of FAI. Understanding the victims is an essential part of understanding the criminal activity. Enhanced awareness, bolstered through a GBA Plus-informed analysis, will be integral to preventing, detecting, and investigating crimes related to FAI. GBA Plus cannot be applied after the fact, but rather, needs to provide a foundation for developing operational training and policy, and planning investigations, intelligence, and engagement activities.

Consultations with Divisions also pinpointed that, while FAI criminal activities target all of Canadian society, there are region-specific differences, shaped by intersecting social, cultural, and economic factors, that impact the vulnerabilities targeted by FAI threat actors, relations between communities and LE, and Canadians' overall FAI threat awareness. Those same intersecting social and cultural factors also means that FAI threat and criminal activities may target and impact different communities based in different geographic regions differently. Examples include the differences in the threat environment between Western and Central Divisions, between smaller Divisions without major urban centres and larger Divisions that contain major urban centres, and the North.

The Way Forward (Low Priority)

19. Collaborate with Divisions to gain further insights on community needs and vulnerabilities in the FAI space.

[APG]

Royal Canadian Mounted Police / Gendarmerie royale du Canada	Security Classification/Designation Classification/désignation sécuritaire **Protected B//For Internal**	Total Pages 22

NOTE: There are existing GBA Plus resources and expertise available, both within the RCMP and other government departments, that can be leveraged to develop training for RCMP personnel to address and unpack potential biases relating to FAI threat actors and activities. This could feed into training development identified above.

[APG]