Elections Canada

PROTECTED B // FOR OFFICIAL USE ONLY

Risk Assessment: Insider Risk GE44

Date: February 19, 2021
Theme: Violent Extremism, Foreign Disruption, Health, Crime
Key Words: Insider threat, accidental, coercion, espionage, sabotage, cyber attack

Executive Summary

- [redacted]

Definitions

- **Insider Risk:** Public Safety defines insider risk "as anyone with knowledge or access to an organization's infrastructure (both physical and computer networks) who maliciously, or by chance, misuses their trusted access to harm the organization's employees, customers, assets, reputation or interests" (Public Safety Canada, 2019).
- **Echo Chamber:** When you are repeatedly exposed to the same information, messages, perspectives, propaganda, and opinions without dissenting perspectives to provide a balanced viewpoint – it is very common on social media (Cota et al., 2019).
- **Phishing**: "is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details or other sensitive details, by impersonating oneself as a trustworthy entity in a digital communication" (Fruhlinger, 2020).
- **Spear-phishing**: "is the act of sending emails to specific and well-researched targets while purporting to be a trusted sender. The aim is to either infect devices with malware or convince victims to hand over information or money" (Swinhoe, 2019).
- **Social engineering**: "is a non-technical strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices. The success of social engineering techniques depends on attackers' ability to manipulate victims into performing certain actions or providing confidential information" (Lord, 2018).
- **Targeted attacks:** "refers to a type of threat in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period" (Ashford, 2019).

- **New Terminology:** Public Safety Canada has shifted its terminology away from terrorism to include three subgroups: religiously motivated violent extremism (RMVE), ideologically motivated violent extremisms (IMVE), and politically motivated violent extremism (PMVE) (CSIS 2019). RMVEs believe they are engaged in a religious struggle that justifies the use of violence, Islamic extremism falls within this grouping. Public safety is moving away from using the terms left and right because many extremist groups have both left and right tendencies. PMVE actors' goals are violently disbanding the government and replacing it with something of their choosing, whereas, IMVEs have personalized complaints they use to justify violence

Risk Assessment

A threat is any potential event or act, deliberate, accidental, or natural hazard, that could cause injury to employees or assets, and thereby affect service delivery adversely. To calculate threat, we ask "what is the intent and capability of the threat?" Do they intend to do us harm, and if so are they actually capable of causing harm?

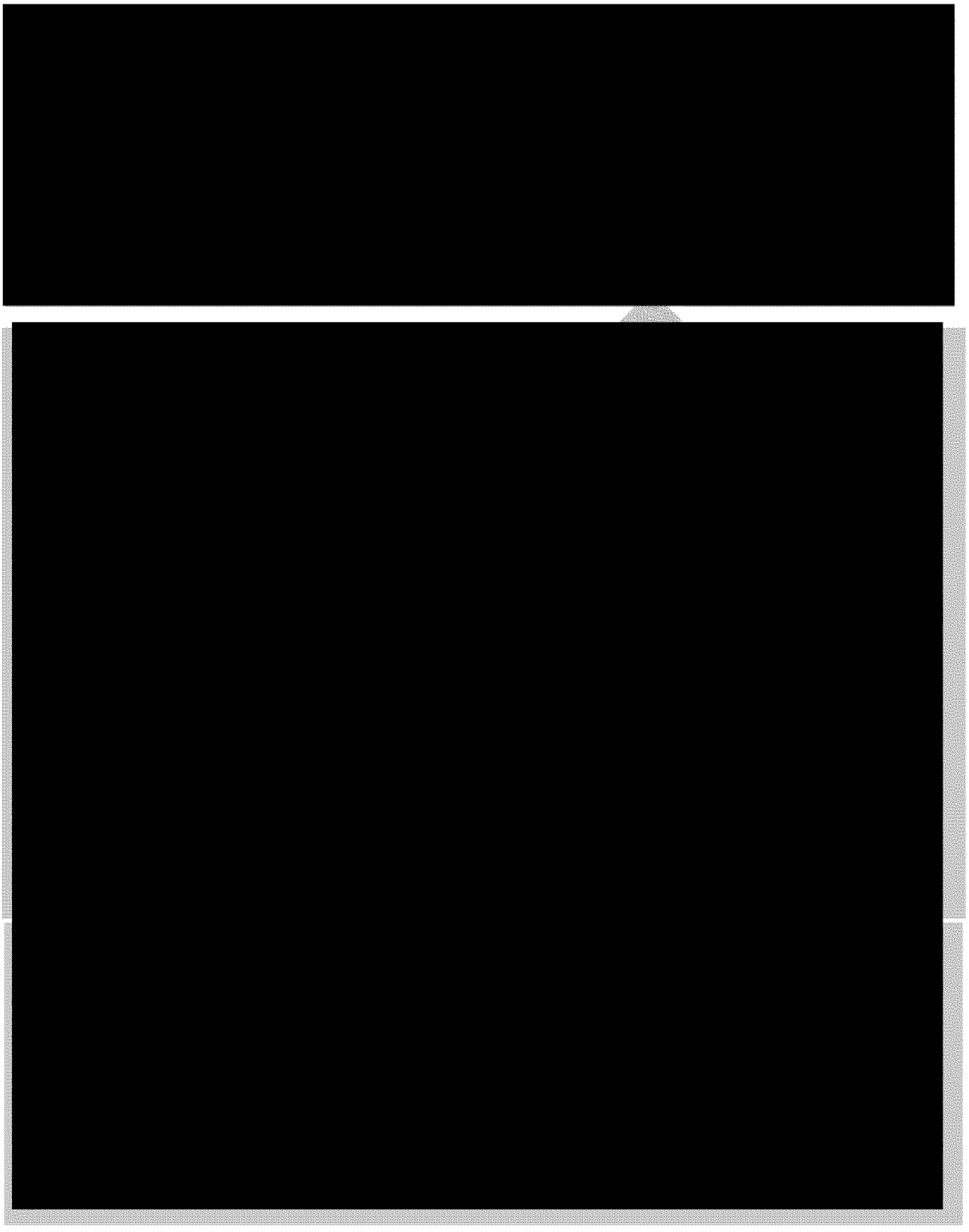
[redacted]

A vulnerability is an inadequacy related to security that could permit a threat to cause injury. To calculate this, we ask "what are the anti-measures and countermeasures we have in place to mitigate the harm?"

Risk is the chance of a vulnerability being exploited, and it is calculated by adding threat and vulnerability together. In addition to open source documents we have leveraged reports from our security partners such as Integrated Terrorist Assessment Centre, CSIS, CSE, Public Safety etc.

[redacted]

Elections Canada



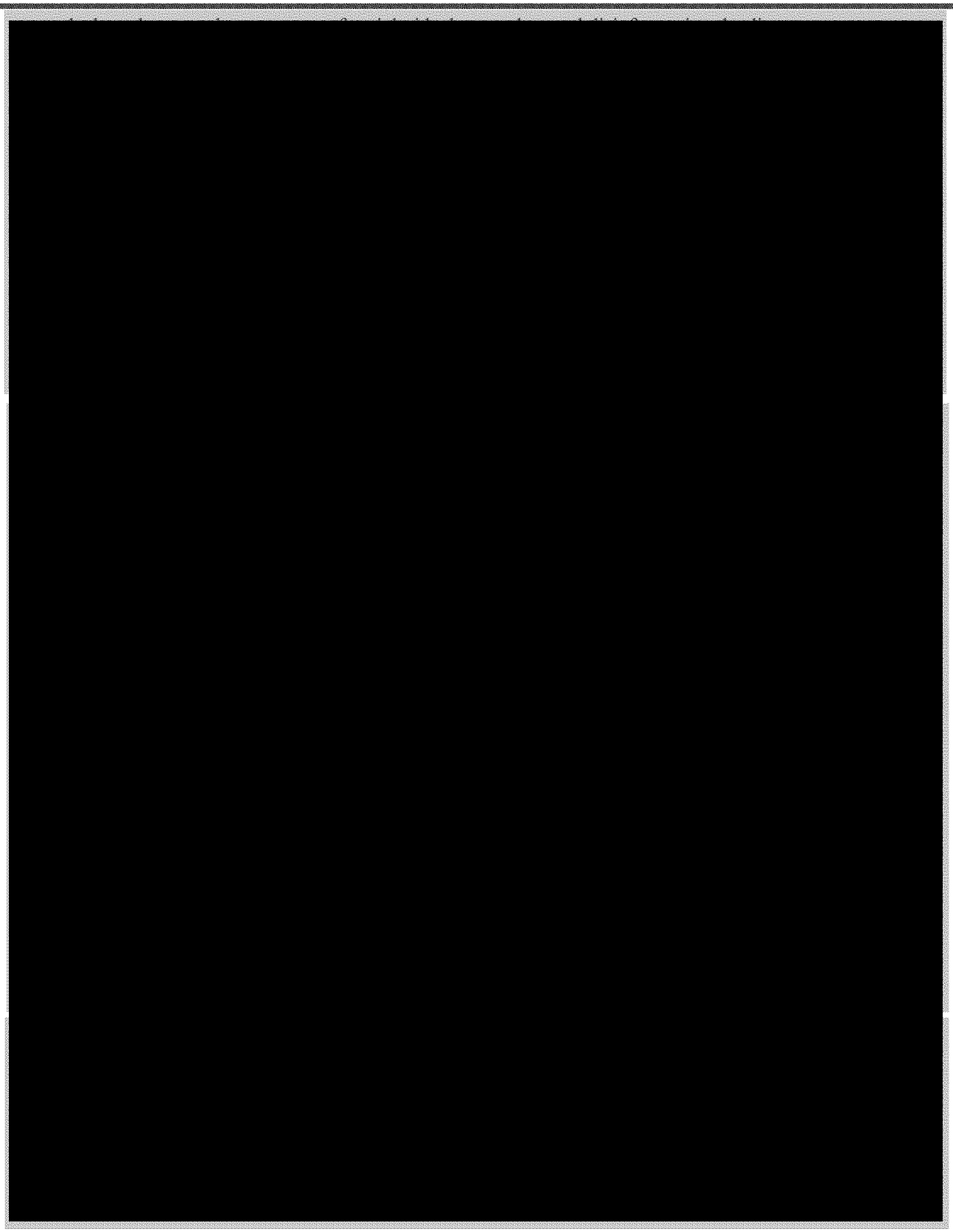
[redacted]

The exploitation of ethnocultural ties to a hostile state is a vulnerability that can be leveraged to advance foreign interests at Canada`s expense. This is often accomplished by threatening members of diaspora communities themselves or their family members living abroad (CSIS 2018: 79). Both Russia and China have used coercive tactics to exploit diaspora communities in Canada, while China has specifically targeted civil servants (CSIS 2018: 79; Marann 2019: 60; Boutilier 2020). Russian intelligence services are also infamous for fabricating compromising information (known as *kompromat*) to coerce businesspeople and government employees in other states (Puusepp 2018: 24-25; Tucker 2017). India and Iran have also employed members of their diasporas in Canada to advance their agendas, with Iran outright harassing and threatening Iranian-Canadians (Berthiaume 2019; Blanchfield 2020).

A common thread among these hostile foreign actors is the appeal to ideology to recruit and influence diaspora communities. States such as Russia amplify populist grievances through rampant disinformation campaigns across various media platforms, and seek to exploit individuals in positions of influence who may become sympathetic to their worldview (GEC 2020: 3). In Europe, both left and right-wing populist parties share similar ideological concerns with Russia over policies of globalization and multilateral institutions, often receiving financial support from the Kremlin (Kolga 2019; Marran 219: 42). With comparable populist political movements emerging in Western Canada and elsewhere, future EC hires may hold ideological beliefs sympathetic to Russian interests, thereby increasing their susceptibility to foreign recruitment. The 2019 NSICOP report warns of an active threat to Canada's political processes by the Russian and Chinese governments through the employment of covert agents within diaspora communities (NSICOP 2019: 62). The Kremlin attempts to recruit Russian-speaking youth by hosting student events and cultural exchanges in Russia, and appeals to their sense of patriotism to garner influence. Once abroad, youth are indoctrinated with pro-Kremlin ideology and groomed as potential candidates for the Russian special services (Puusepp 2018: 9). China also appeals to nationalism in its recruitment efforts. Given the CCP's recently adopted National Intelligence Law granting it sweeping powers to request information from all Chinese citizens, expats working for EC and other government agencies may feel compelled to comply with foreign intelligence efforts when framed as a matter of national duty (CSIS 2018: 85; NSICOP 2019: 60).

[redacted]

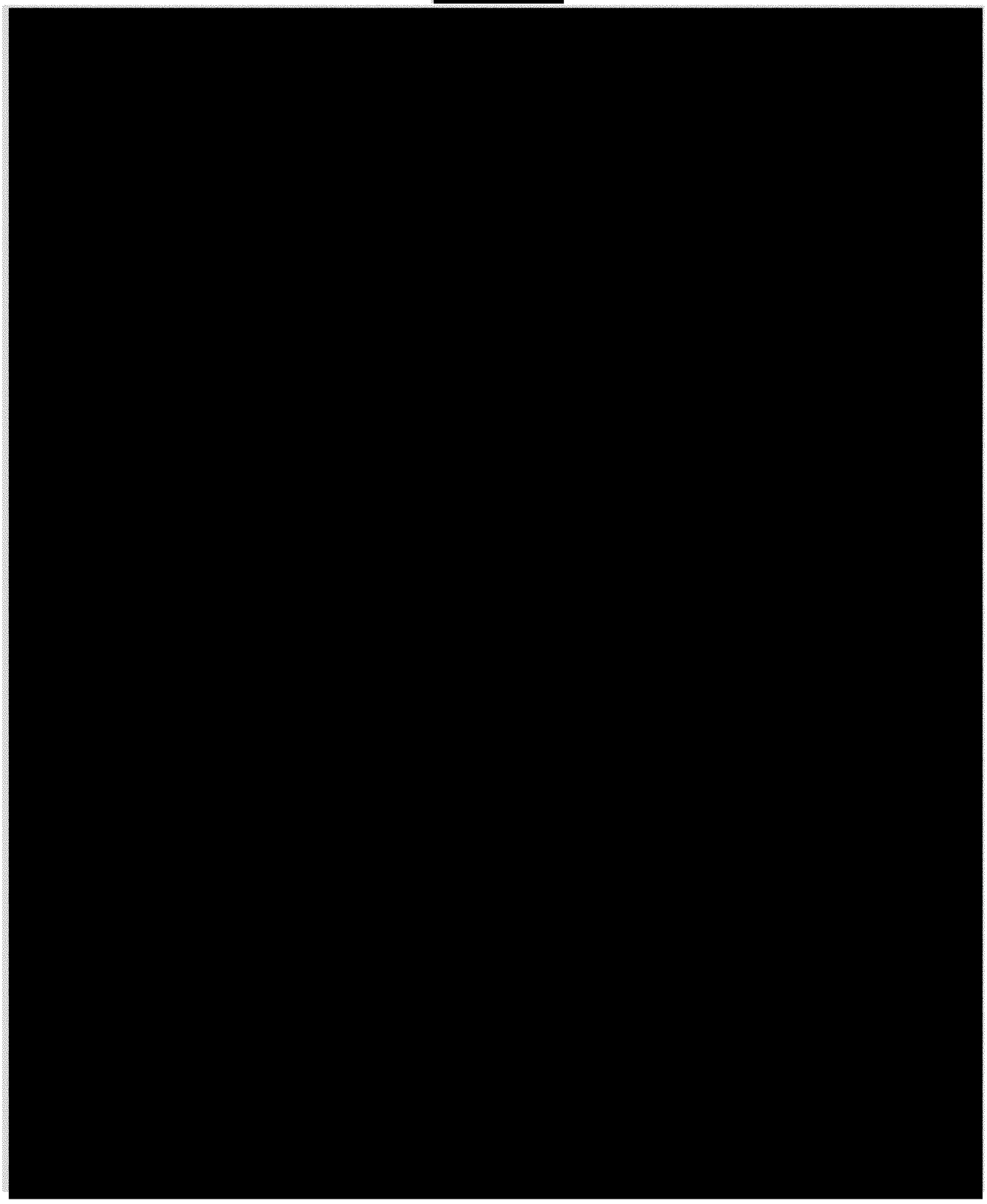
Elections Canada



Elections Canada

Elections Canada

[redacted]



Elections Canada

[redacted]

Elections Canada

[redacted]