Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions | Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Overview Report:

Summary of *Countering Foreign Interference Act* (Bill C-70)

Prepared by: Commission Counsel

Summary of Report

This Overview Report summarizes Bill C-70, *An Act Respecting Countering Foreign Interference*, as enacted, and describes the Bill's progress through Parliament. This legislation is now known as the *Countering Foreign Interference Act*.

Note to Reader

Pursuant to Rules 42-44 of the Commission's *Rules of Practice and Procedure*, the following Overview Report contains a summary of background facts and documents relating to the Commission's mandate.

Overview Reports allow facts to be placed in evidence without requiring the facts and related documents to be presented orally by a witness during the public hearings. Overview Reports may be used to assist in identifying issues relevant to the Commission, make findings of fact and enable recommendations to be made by the Commission.

Parties have been provided an opportunity to comment on the accuracy of this Overview Report. Commission Counsel and the Parties may call evidence from witnesses at the Inquiry that casts doubt on the accuracy of the content of the documents underlying this Report. The Parties may also make submissions regarding what, if any, weight should be given to this Report and the cited documents.

Contents

1. Introduction

[1] This Overview Report summarizes Bill C-70, *An Act Respecting Countering Foreign Interference*, as ultimately enacted by Parliament.[1] This legislation is now known as the *Counting Foreign Interference Act*. It also describes the Bill's progress through Parliament.

[2] Bill C-70 enacted the *Foreign Influence Transparency and Accountability Act* ("***FITAA***") and amended the:

a. *Canadian Security and Intelligence Service Act*, R.S.C., 1985, c. C-23 ("***CSIS Act***")

b. *Security of Information Act*, R.S.C., 1985, c. O-5 ("***SOIA***")

c. *Criminal Code*, R.S.C., 1985, c. C-46

d. *Canada Evidence Act*, R.S.C., 1985, c. C-5

e. *Immigration and Refugee Protection Act*, S.C. 2001, c. 27 ("***IRPA***")

[3] On 20 June 2024, Bill C-70 received Royal Assent. Amendments to the *CSIS Act* came into effect on that day. Amendments to *SOIA*, the *Criminal Code* and the *Canada Evidence Act* came into force on 19 August 2024 (60 days after Royal Assent).

[4] *FITAA* will come into force on a day fixed by order in council. Public Safety Canada ("**Public Safety**") estimates the Foreign Influence Transparency Registry will take a year to set up.

[1] *An Act respecting countering foreign interference*, S.C. 2024, c. 16, **COM0000381**.

2. Summary of Bill C-70

2.1 Part 1 – Amendments to the *CSIS Act*

[5] Part 1 of Bill C-70 amended the *CSIS Act* in five major ways.

Datasets

[6] First, there are amendments about the definition, collection, evaluation, retention, disclosure, querying and exploitation of datasets.

[7] The dataset regime was introduced into the *CSIS Act* in 2019 to provide a legal framework for CSIS to collect, retain and analyze large quantities of data not directly and immediately related to a threat. The dataset rules were a legislative response to a 2016 Federal Court decision finding CSIS did not have the lawful authority to retain and exploit large amounts of electronic metadata incidentally collected by the Service.[2]

[8] Bill C-70 made numerous changes to the detailed rules governing CSIS's use of datasets.

Definitions (section 11.01)

[9] Definitions of "Canadian," "dataset," "exploitation" and "query" were removed from section 2 of the *CSIS Act* and reintroduced with some modifications in section 11.01, which clarifies these definitions apply only to the dataset authority in the Act.

[10] The new "dataset" definition incorporates the elements of the original definition and clarifies the scope of the dataset authority, to ensure it does not apply to information to which sections 12 to 16 apply. The definition removes reference to "directly and immediately related to a threat," as not all of CSIS' functions are related to threats to the security of Canada. The definition also specifies the term "dataset" only applies to collections of information with personal information, formerly a requirement located in

[2] *X (Re)*, 2016 FC 1105.

section 11.02. Personal information is no longer limited to information that does not relate to activities representing a threat to the security of Canada.[3]

[11] The definition of "exploitation" clarifies that it includes a series of computational analyses, as well as a single computational analysis.

[12] The definition of "query" clarifies that a query can include a series of specific searches as well as a single specific search.

Datasets classes

[13] The Minister of Public Safety and Emergency Preparedness ("Minister") no longer has to annually, by order, determine classes of Canadian datasets for which collection is authorized (section 11.03(1)). An order is valid for up to two years (section 11.03(2.1)).

[14] The Minister may determine a class of Canadian datasets is authorized for collection if they conclude that querying or exploiting the datasets in the class could lead to results relevant to CSIS's duties and functions under section 12, 12.1, 15 or 16. Previously, section 15 was not included.

Dataset collection

[15] If CSIS concludes the information collected under section 12, 15 or 16 constitutes a dataset or could be used to constitute a dataset, the information is deemed collected as a dataset under section 11.05 (section 11.051).

[16] As soon as feasible after collecting a dataset outside of Canada under section 11.05, CSIS must destroy it or provide it to a designated employee under section 11.07 (section 11.052).

[17] If CSIS concludes information incidentally collected in the execution of a warrant (under section 21 or 22.21 or a production order under section 20.4) constitutes a dataset or could be used to constitute one, the information is deemed collected as a dataset under

[3] The other elements of the definition still apply: a collection of information containing "personal information" as defined in section 3 of the *Privacy Act*, R.S.C. 1985, c. P-21, stored as an electronic record and characterized by a common subject matter (*CSIS Act*, ss 2, 11.02).

section 11.05 and the terms and conditions of the warrant or production order apply (section 11.053).

[18] Datasets deemed collected on more than one day under sections 11.051, 11.052, 11.053 or 22.1(3) are deemed collected on the latest date for the purposes of section 11.07 (section 11.054).

Dataset evaluation

[19] The Director of CSIS ("**Director**") may delegate the designation power in section 11.06(1) (section 11.06(1.1)).[4]

[20] The time for a designated employee to evaluate a dataset and confirm the following is extended from 90 to 180 days (section 11.07(1)):

a. The dataset was publicly available at the time of collection, and

b. The dataset predominantly relates to:

i. individuals within Canada or Canadians,

ii. individuals who are not Canadians and who are outside Canada, or

iii. non-Canadian corporations who are outside Canada.

[21] If foreign datasets include information relating to individuals within Canada or Canadians and CSIS decides to treat it as a Canadian dataset, that dataset is deemed a Canadian dataset (section 11.07(1.1)).

[22] Section 11.08 only applies if datasets did not belong to an approved class on the day of collection, instead of whether they did not belong to an approved class at any time (sections 11.07(2), 11.08(1), 11.08(2)).

[23] To determine whether a dataset being evaluated has been previously collected, a designated employee may compare the dataset to other CSIS datasets (section 11.07(3.1)). This is the case whether or not the dataset's retention has been authorized.

[4] The designation power allows the Director to designate employees to carry out activities in sections 11.07, 11.2 and 11.22.

[24] During the evaluation period, a designated employee deletes irrelevant "personal information" as defined in section 3 of the *Privacy Act*, R.S.C. 1985, c. P-21, and not "any information that relates to personal information" (section 11.07(6)(a)). This was not a change to the obligation, but a correction to align the French and English versions of the provision.

Dataset retention

[25] The process in section 11.09 for applications to retain a dataset applies to deemed Canadian datasets and datasets confirmed by a designated employee and must be submitted before the evaluation period expires (section 11.09(1)).

[26] With respect to section 11.1 and information in Canadian datasets with a reasonable expectation of privacy relating to the physical or mental health of someone, information in Canadian datasets subject to solicitor-client privilege or the professional secrecy of advocates and notaries, and information in foreign datasets that by its nature or attributes relates to a Canadian or person in Canada:

a. CSIS is only required to "take reasonable measures to ensure" it deletes or removes this information (section 11.1(1)). Previously it had to do so.

b. Section 11.1(2), which stipulates what happens to information removed from a foreign dataset, no longer applies to information retained under section 11.21(1).

[27] When the Director (or designate) requests the Minister's approval to apply for a judicial authorization, they shall indicate the class to which a Canadian dataset belonged at the time of collection, or if a request was made for a new class under section 11.08(1)(b), the class to which it belongs (section 11.12(2)(a)).

[28] A judge may authorize retention of a Canadian dataset if satisfied that retention is likely to assist CSIS in the performance of its duties or functions under sections 12, 12.1, 15 and 16 (section 11.13(1)(a)). Previously section 15 was not included in this criterion.

[29] In relation to expiring judicial authorization to retain datasets, if CSIS does not request or obtain the Minister's approval under section 11.12 to make a new application for a

judicial authorization to retain a Canadian dataset before the existing judicial authorization expires, then CSIS must destroy the dataset (sections 11.15(3), (3.1), (4)).

[30] This contrasts to the previous regime where CSIS had to actually file its application before expiry of the authorized retention period.

Dataset disclosure

[31] CSIS can disclose publicly available datasets. If it does so, section 19 does not apply to the disclosure (section 11.11(3)).

[32] An application for judicial authorization must set out the way CSIS intends to disclose the dataset (section 11.13(2)(b.1)). Judicial authorizations issued under section 11.13 must have terms and conditions necessary for disclosure of the dataset (section 11.14(1.1)) and are valid for up to five years (previously it was two) (section 11.14(2)). Disclosure of datasets retained by judicial authorization is not subject to section 19 (section 11.14(1.2)).

[33] Ministerial authorization for retention of foreign datasets must have terms and conditions necessary for disclosure of the dataset (section 11.17(2.1)) and are valid for up to 10 years (previously it was 5) (section 11.17(3)). Disclosure of datasets retained under ministerial authorization is not subject to section 19 (section 11.14(2.2)).

Dataset query or exploitation

[34] Authority for a designated employee to query or exploit, to the extent it is strictly necessary, a Canadian dataset is extended to assisting CSIS in the performance of its duties and functions under section 15 (sections 11.2(2), (3)). Previously it only applied to performance of CSIS duties and functions under section 12 or 12.1.

[35] Authority for the Director to authorize a designated employee to query a Canadian or foreign dataset without valid authorization if the dataset was collected under subsection 11.05 and there are exigent circumstances, is extended to authorizing exploitation of the dataset (section 11.22(1)) and retention of that exploitation (section 11.22(2.1)). Previously section 11.22 only referred to querying a dataset.

[36] If a query or exploitation was done based on exigent circumstances under section 11.22, CSIS must give NSIRA a copy of the Director's authorization and indicate the

results of the query or exploitation and any actions taken (section 11.25(c)). Previously the section only required this if there was a query.

Collection outside of Canada

[37] Second, section 16, which sets out CSIS's mandate to assist in the collection of information relating to foreign states and persons within Canada, was amended to include the **collection, from within Canada, of information or intelligence located outside Canada** if the assistance is directed at a person or thing in Canada or at an individual who was in Canada but is temporarily outside Canada (section 16(1.1)). Before amendment, the Federal court and Federal Court of Appeal held collection was limited to information located within Canada.

Sharing information

[38] Third, section 19, which describes when CSIS can disclose information it obtains under its duties and functions, was expanded to authorize CSIS to **share information with a broader audience**:

a. Where information may be used in the investigation of any Canadian law, CSIS can disclose information to "any person" having jurisdiction (section 19(2)(a)). Previously, it was to a peace officer having jurisdiction.

b. CSIS can disclose information to "any person or entity" where the Minister opines doing so is essential in the public interest and the public interest clearly outweighs any invasion of privacy that could result from the disclosure to that person or entity (section 19(2)(d)).

[39] CSIS can disclose information to any person or entity for the purpose of building resiliency against threats to the security of Canada as long as three criteria are met (section 19(2.2)). The information must:

a. Have already been provided to a federal department or agency that performs duties and functions to which the information is relevant.

b. Not contain any personal information, as defined in section 3 of the *Privacy Act*, of a Canadian citizen, a permanent resident or any individual

in Canada, other than personal information of the individual to whom the information is disclosed.

c. Not contain the name of a Canadian corporation or the name of a Canadian entity, other than the name of the corporation or entity to which the information is disclosed.

Judicial controls

[40] Fourth, judicial controls under the *CSIS Act* (Part II) were variously amended.

[41] CSIS can apply for judicial preservation and production orders (sections 20.3 and 20.4, respectively).

[42] The warrant application process allows a judge to authorize collection, from within Canada, of information or intelligence located outside Canada (section 21(3.2)). (Section 21 allows CSIS to apply for warrants to enable it to investigate, within or outside Canada, a threat to the security of Canada or to perform its duties and functions under section 16.)

[43] CSIS can apply for a warrant to obtain information, record, document or thing (sections 22.21, 24). (Section 22.21 allows CSIS to apply for warrants to enable it to investigate, within or outside Canada, a threat to the security of Canada or to perform its duties and functions under section 16.)

[44] Assistance orders are extended to apply to warrants issued under sections 22.21 and 23, as well as sections 21, 21.1 (section 22.3(1)).

[45] There is a more comprehensive and prescribed process for warrants authorizing removal of any thing from where it was installed in the performance of CSIS's duties and functions under section 12 or 16 or in accordance with a warrant under section 21, 21.1 or 22.21 (section 23).

[46] The circumstances in which CSIS can apply for a warrant to remove a thing from the place where it was installed are expanded (sections 23-24, 27).

[47] In addition to being heard in private and in accordance with regulations under section 28, applications under section 11.3, 20.3, 20.4, 21, 21.1, 22, 22.1, 22.21, 22.3 or 23 will also be made *ex parte* (section 27).

Parliamentary review

[48] Fifth, there is now a mechanism for parliamentary review of the *CSIS Act* every five years (section 29).

2.2 Part 2 – Amendments to *SOIA* and the *Criminal Code*

[49] Part 2 amended *SOIA* and the *Criminal Code*, creating the following offences in *SOIA*, which is now renamed the *Foreign Interference and Security of Information Act* ("***FISOIA***"):

a. **Foreign-influenced intimidation, threats or violence**: section 20 of *SOIA* was amended in *FISOIA* to criminalize foreign-influenced intimidation, as well as threats or violence. Where the offence takes place in Canada or involves people with specified links to Canada, it no longer requires proof the prohibited act was for the purpose of increasing the capacity of the foreign entity to harm Canadian interests or was reasonably likely to harm Canadian interests. Proof of such purpose or harm is still required if the offence is committed outside Canada and the requirements in section 20(2) are not present.

b. **Commission of an indictable offence for a foreign entity**: section 20.2 of *FISOIA* is a new offence of committing an indictable offence at the direction of, for the benefit of, or in association with a foreign entity. It is like existing offences addressing terrorism and organized crime in the *Criminal Code*.

c. **Conduct or omission for a foreign entity**: section 20.3 of *FISOIA* is a new general foreign interference offence, which applies where a person knowingly engages in surreptitious or deceptive conduct or omits, surreptitiously or with the intent to deceive, to do anything at the direction of, for the benefit of, or in association with a foreign entity. The

prosecution must prove the person's conduct or omission was for a purpose prejudicial to the safety or interests of Canada, or the person was reckless as to whether their conduct or omission would cause such prejudice.

d. **Political interference for a foreign entity:** section 20.4 of *FISOIA* is a new offence of engaging in surreptitious or deceptive conduct at the direction of, or in association with, a foreign entity, with the intent to influence a Canadian political or governmental process or to influence the exercise of a democratic right in Canada.[5]

[50] All offences are punishable by a maximum penalty of life in prison and sentences would be consecutive to any other sentence other than life imprisonment. Senior Counsel for the Department of Justice ("**DoJ**") told the House of Commons Standing Committee on Public Safety and National Security ("**SECU**") that the mandatory consecutive sentences mirror provisions for terrorism and organized crime in the *Criminal Code* to reflect the seriousness of foreign interference offences.[6]

[51] Preparatory acts to most *FISOIA* offences are criminalized and the maximum penalty was increased from two to five years (section 22).

[52] Bill C-70 changes the definition of "special operational information" in *SOIA* (section 8(1)) to address inappropriate sharing of military technology and knowledge.[7]

---

[5] The non-exhaustive definition of "political or governmental process" is found in the *Foreign Influence, Transparency and Accountability Act*, enacted by Bill C-70. The Foreign Influence and Transparency Commissioner will interpret and apply the definition, but according to officials from the Ministry of Public Safety and Emergency Preparedness, the definition is intended to include a political party's nomination process, party leadership contests and appointments and elections within a political party: SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**, 9:35-9:40. See also SECU-114 (June 10, 2024), **COM0000426(EN)/COM0000432(FR)**, 16:25.

[6] SECU-114 (June 10, 2024), **COM0000426(EN)/COM0000432(FR)**, 16:10.

[7] SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**, 8:25.

[53] Bill C-70 made certain provisions in the *Criminal Code* about the interception of private communications apply to certain offences in *FISOIA* (sections 185(1.1)(a), (b.1), 186(1.1)(a), (b.1), 186.1(1)(a), (b.1), 196(5)(a), 196.1(a), (b.1)).

[54] The *Criminal Code* was amended by replacing the sabotage offence (section 52) requirement of "a purpose prejudicial to" with "the intent to endanger" and adding two companion offences: sabotage of essential infrastructure (section 52.1) and the making, possession or distribution of devices designed to be used for sabotage (section 52.2). Prosecution requires consent of the attorney general.

[55] "Essential infrastructure" is defined in section 52.1(2) as a facility or system, public or private, completed or under construction, providing or distributing, or intending to, services essential to the health, safety, security or economic well-being of persons in Canada, including the following:

a. Transportation infrastructure,

b. Information and communication technology infrastructure,

c. Water and wastewater management infrastructure,

d. Energy and utilities infrastructure,

e. Health services infrastructure,

f. Food supply and food services infrastructure,

g. Government operations infrastructure,

h. Financial infrastructure, and

i. Any other infrastructure prescribed by regulation.[8]

[8] SECU, 44th Parliament, 1st Session, Report 13 (June 10, 2024), **COM0000419(EN)/COM0000420(FR)**; *An Act respecting countering foreign interference*, S.C. 2024, c. 16, **COM0000381**.

2.3 Part 3 – A New Regime Governing Disclosure and Use of Sensitive Information in Federal Court

[56] Part 3 of Bill C-70 established a secure administrative review proceedings regime governing the disclosure, protection and use of sensitive or potentially injurious information in administrative proceedings before the Federal Court or Federal Court of Appeal (*Canada Evidence Act*, sections 38.2, 38.21-38.45).[9] This regime replaces all existing stand-alone regimes[10] except for the scheme under the *Immigration and Refugee Protection Act* (*IRPA*) and applies to administrative contexts currently without a regime. Judicial review of decisions made under the new *Foreign Influence, Transparency and Accountability Act (FITAA)*, discussed in the next section, will be done in Federal Court and so also will be subject to this new regime.

[57] Under the new regime, if a participant in a proceeding expects sensitive or potentially injurious information could be disclosed, they must give notice to the Attorney General of Canada ("**AGC**") (sections 38.2 to 38.31). If the AGC does not authorize disclosure, the matter is brought before the judge hearing the judicial review or appeal. The judge decides whether disclosure of the sensitive information would be injurious to international relations, national defence or national security (section 38.25 to 38.26). If the judge concludes disclosure would not be injurious to international relations, national defence or national security, then they may order disclosure. If the judge concludes disclosure would be injurious but the public interest in disclosure outweighs the public interest in non-disclosure, they may order disclosure subject to any conditions they consider appropriate. If the judge concludes disclosure would be injurious to

[9] In s 38.2, "sensitive information" is information relating to international relations, national defence or national security that the federal government is taking measures to safeguard and "potentially injurious information" means information that could injure international relations, national defence or national security.

[10] Judicial review of listing of terrorist entities based on sensitive information in the *Criminal Code*; issuance of a no-fly list based on sensitive information under the *Secure Air Travel Act*, S.C. 2015, c. 20; and passport refusal or cancellation based on sensitive information under the *Prevention of Terrorist Travel Act*, S.C. 2015, c. 36.

international relations, etc., then they must order confirmation of the prohibition on disclosure.

[58] Part 3 of Bill C-70 also amended the *Canada Evidence Act* (sections 37.1, 38.09) to bar an accused's interlocutory appeal about non-disclosure. An accused can only appeal **after** they are convicted, unless there are exceptional circumstances justifying an earlier appeal. The Crown can still appeal an order for disclosure on an interlocutory basis.

[59] If an order or decision is made under the *Canada Evidence Act* under the above procedure, or made under any other federal law, and would result in disclosure, the AGC can issue a certificate prohibiting its disclosure. The certificate is reviewable by the Federal Court of Appeal.

[60] There is also a process dealing with the use of sensitive information by the judge in making their decision on the merits of the federal proceeding (sections 38.32 to 38.42). The judge can appoint a special counsel to protect the interests of a non-governmental party to the proceedings (sections 38.2, 38.34 to 38.38).

[61] Section 487.3 of the *Criminal Code* lists factors a judge must consider when determining whether to deny access to, and prohibit the disclosure of, any information presented to the court to obtain a warrant. The factors are expanded to include whether disclosure would be injurious to international relations, national defence or national security. *IRPA* is similarly amended to provide for the protection of information relating to international relations and national defence (sections 77, 79.1, 82.31, 83, 85.1, 86.1, 87.01).

[62] In parallel with the above process, Bill C-70 also changed the *Criminal Code* and *IRPA*, to protect sensitive information in criminal and *IRPA* security certificate proceedings if disclosure would be injurious to international relations, national defence or national security (*Criminal Code*, section 487.3(2)(a); *IRPA*, sections 77(2), 79.1(1), 83.31(1), 83(1)(c), (d), (e), 83(1.2)(c), 85.1(2)(a), 86.1(1), 87.01(1)).

2.4 Part 4 – Foreign Influence Transparency and Accountability Act (*FITAA*)

Summary of *FITAA*

[63] Part 4 enacted *FITAA*, which:

a. Creates a Foreign Influence Transparency Registry.

b. Provides for Governor in Council appointment of a Foreign Influence Transparency Commissioner ("**FITC**") after consultation with parliamentarians[11] and approval by resolution of the Senate and House of Commons.[12]

c. Requires registration of persons or entities who enter an **arrangement with a foreign principal**. Such an arrangement exists where all the following elements are present:[13]

   i. A person or entity undertakes to carry out any of the following activities:

      - Communicates with a **public office holder**.[14]
      - Communicates, disseminates or causes to be communicated or disseminated, information related to the political or governmental process.

---

[11] Under *FITAA*, s 9(2)(a), before appointing the FITC, the Governor in Council must consult with the Leader of the Government in the Senate or Government Representative in the Senate; the Leader of the Opposition in the Senate; the Leader or Facilitator of every other recognized party or parliamentary group in the Senate; the Leader of the Opposition in the House; and the leader in the House of Commons of each party with at least 12 members in the House.

[12] *FITAA*, s 9(2)(b).

[13] *FITAA*, s 2 (definition of "arrangement").

[14] *FITAA*, s 2 defines "public officer holder" as an individual included in a class of individuals specified in the regulations and, unless excluded by the regulations, any of the following individuals: (a) a public office holder as defined in the *Lobbying Act*, R.S.C. 1985, c. 44 (4th Supp.), ss 2(1); (b) an individual referred to in any of ss 4(1)(a) to (c) of the *Lobbying Act*; (c) an individual referred to in ss 4(1)(d) or (d.1) of the *Lobbying Act*; (d) an officer or employee of an entity referred to in ss 4(c)(ii) of *FITAA*.

- Distributes money or items of value or provides a service or the use of a facility.[15]

ii. The activities are in relation to a **political or governmental process**[16] of federal, provincial, territorial, municipal or Indigenous governments.

iii. The activities are under the direction of, or in association with, a **foreign principal**.[17]

d. Requires the FITC to establish and maintain a public registry with information about foreign influence arrangements.[18]

e. Requires the FITC report annually to the Minister of Public Safety who must table the FITC's annual reports in each House of Parliament.[19]

f. Gives the FITC tools to administer and enforce the *FITAA*, including:

i. Powers to investigate, including receiving information that would not be admissible in court.[20]

ii. Several new offences (e.g. the offence of failing to report the required information).[21]

---

[15] *FITAA*, ss 4-7, 33-35; SECU-109 (30 May 2024), **COM0000421(EN)/COM0000427(FR)**, 8:15.

[16] *FITAA*, s 2 defines "political or governmental processes" as including: (a) any proceeding of a legislative body; (b) the development of a legislative proposal; (c) the development or amendment of any policy or program; (d) the making of a decision by a public office holder or government body, including the awarding of a contract; (e) the holding of an election or referendum; and (f) the nomination of a candidate or the development of an electoral platform by a political party.

[17] *FITAA*, s 2 defines a "foreign principal" as an economic entity, a foreign entity, a foreign power or a foreign state, as those expressions are defined in subsection 2(1) of the *Security of Information Act*.

[18] *FITAA*, s 8.

[19] *FITAA*, ss 28-30.

[20] *FITAA*, s 16.

[21] *FITAA*, ss, 23-25. If convicted on indictment, a person can be fined up to $5 million or sentenced to five years in prison or both. On summary conviction, a person can be fined up to $200,000 or two years less a day in prison or both.

iii. Power to issue notices of violation (if the FITC has reasonable grounds to believe a violation has been committed) with administrative monetary penalties.[22]

g. Provides for a mandatory review of *FITAA* in the first year after a general election, which requires the Minister of Public Safety, within 120 days of the review report's submissions to Parliament, to table a response addressing each recommended change.[23]

[64] The FITC must decide whether to proceed with a notice of violation or a criminal prosecution, as each proceeding precludes the other.

[65] The Registry will require regulations including the types of information required, the kind of information the FITC must publish online, the amount of administrative monetary penalties and parameters for sharing information with other agencies.[24]

[66] The Governor in Council can specify and exclude classes of individuals for the purposes of the definition of "public office holder" in section 2[25] and exclude classes of individuals subject to section 5 by regulation.[26] Arrangements can also be excluded by regulation.[27]

[67] The activities of the FITC are subject to review by the National Security and Intelligence Review Agency.[28] Decisions made by the FITC are reviewed by the Federal Court.[29]

[68] Public Safety's priority is to have the *FITAA* registry in place before the next federal election. Public Safety estimates the registry will take a year to set up.[30]

---

[22] *FITAA*, ss 18-22.

[23] *FITAA*, ss 31, 32.

[24] *FITAA*, s 27.

[25] *FITAA*, ss 27(a), (b).

[26] *FITAA*, s 6(1)(c).

[27] *FITAA*, s 6(2)(b).

[28] *National Security and Intelligence Review Agency Act*, S.C. 2019, c. 13, s 2, definition of "department."

[29] *FITAA*, s 26.

[30] SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**, 8:30-8:35, 9:00; Minister Dominic LeBlanc, SECU-113 (June 6, 2024), **COM0000425(EN)/COM0000431(FR)**, 9:20.

Government's intended application of *FITAA*

[69] Representatives from Public Safety, CSIS and DoJ testified several times during SECU's study of Bill C-70. They spoke to government's intended application of *FITAA*.

[70] The Public Safety Associate ADM, National and Cybersecurity, told SECU that *FITAA* is intended to promote openness and transparency and to deter, and introduce consequences for, those who seek to exert influence in non-transparent ways.[31] The focus of the Registry is transparency in the public domain around activities to change public opinion or influence a governmental process.[32]

[71] The Public Safety Director General, said the definition of "arrangement" in *FITAA* is intended to include a verbal understanding and does not require a written contract[33] or the payment of money.[34] The use of "in association with" or "under the direction of" with the term "arrangement" is intended to communicate some form of understanding or agreement between an entity doing the influencing and the foreign power.[35]

[72] The intent is to make the criteria sufficiently broad to capture any type of arrangement with a foreign state. It will be up to the FITC to determine whether the threshold is met. Nevertheless, it will require some degree of understanding between a foreign state and an individual or an entity that has an arrangement. It cannot be just somebody doing it because they think the foreign power would like them to be doing it. There must be some degree of understanding between the person and the state and some link between the activity and the state. There would have to be some understanding that the influence or the activity that is being undertaken is being done for the state, i.e. an understanding of the linkages between the activity and the state, and an agreement to do this for the state.[36]

---

[31] SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**, 8:15.

[32] SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**, 8:50.

[33] SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**, 8:55, 9:35; See also SECU-113 (June 6, 2024), **COM0000425(EN)/COM0000431(FR)**, 9:15.

[34] SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**, 9:30.

[35] SECU-113 (June 6, 2024), **COM0000425(EN)/COM0000431(FR)**, 9:40.

[36] SECD Meeting 57 (June 12, 2024), **COM00004443,** 57:25-57:26.

[73] The Director General also said the definition of "political or government process" is a non-exhaustive list[37] and government intended it to include a political party's nomination process,[38] party leadership contests and appointments and elections within a political party.[39] It also applies to Crown corporations.[40] However, although the definition is not exhaustive, the application of *FITAA* is limited to federal, provincial, municipal and Indigenous political or governmental processes.

[74] With respect to investigative powers, Public Safety and CSIS officials said the FITC can receive intelligence from security and intelligence agencies but there may be limits on the use of it[41] and there will have to be a memorandum of understanding or other process for information sharing between CSIS and the FITC.[42]

[75] The FITC will have the ability to issue interpretation bulletins to explain what they may consider registerable activities. One key component of the FITC's work is educating the public on their obligations.[43]

3. Progress of Bill C-70

[76] Bill C-70 went through first reading on 29 May 2024, and that same day the House referred it to the Standing Committee on Public Safety and National Security ("**SECU**").[44]

---

[37] SECU-114 (June 10, 2024), **COM0000426(EN)/COM0000432(FR)**, 16:35. See also SECU-114 (June 10, 2024), **COM0000426(EN)/COM0000432(FR)**, 16:30.

[38] SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**, 9:40. See also SECU-114 (June 10, 2024), **COM0000426(EN)/COM0000432(FR)**, 16:25.

[39] SECU-113 (June 6, 2024), **COM0000425(EN)/COM0000431(FR)**, 9:35. See also SECU-114 (June 10, 2024), **COM0000426(EN)/COM0000432(FR)**, 16:25.

[40] SECU-113 (June 6, 2024), **COM000425(EN)/COM0000431(FR)**, 17:20.

[41] SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**, 10:05.

[42] SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**, 10:05; See also SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**, 10:05.

[43] SECD Meeting 57 (June 12, 2024), **COM0000443** 57:25.

[44] House of Commons, 44th Parliament, 1st Session, *Debates*, Vol 151, No 320 (May 29, 2024), **COM0000390(EN)/COM0000391(FR)**.

[77] SECU heard from 52 witnesses, received 13 written submissions and reviewed Bill C-70 clause-by-clause.[45] On 10 June 2024, SECU adopted Report 13, which it presented to the House on 11 June.[46] SECU recommended some substantive amendments.

[78] On 12 June 2024, the House unanimously adopted SECU's amendments and concurred in Bill C-70 at the report stage, with the addition of one more amendment clarifying that authorized disclosure by CSIS for the purpose of building resiliency against threats allows disclosure of the name of the corporation or entity to which information is disclosed (*CSIS Act*, section 19(2.1)(c)).[47]

[79] House debate at third reading concluded on 12 June 2024.[48] The House unanimously voted to pass Bill C-70 on 13 June.[49]

[80] On 5 June 2024, the Senate authorized its National Security, Defence and Veterans Affairs Standing Committee ("**SECD**") to study Bill C-70 before it went to the Senate.[50] SECD heard from 35 witnesses from 26 organizations in June 2024, (10th, 12th and 13th) with many of the same people testifying as at SECU.[51]

---

[45] SECU-109 (May 30, 2024), **COM0000421(EN)/COM0000427(FR)**; SECU-110 (June 3, 2024), **COM0000422(EN)/COM0000428(FR)**; SECU-111 (June 4, 2024), **COM0000423(EN)/COM0000429(FR)**; SECU-112 (June 5, 2024), **COM0000424(EN)/COM0000430(FR)**; SECU-113 (June 6, 2024), **COM0000425(EN)/COM0000431(FR)**; SECU-114 (June 10, 2024), **COM0000426(EN)/COM0000432(FR)**.

[46] SECU, 44th Parliament, 1st Session, Report 13 (June 10, 2024), **COM0000419(EN)/COM0000420(FR)**; *An Act respecting countering foreign interference*, S.C. 2024, c. 16, **COM0000381**.

[47] House of Commons, 44th Parliament, 1st Session, *Journals*, No 330 (June 12, 2024), **COM0000442** and *Debates*, Vol 151, No 330 (June 12, 2024), **COM0000392(EN)/COM0000393(FR)**, 16:05.

[48] House of Commons, 44th Parliament, 1st Session, *Debates*, Vol 151, No 330 (June 12, 2024), **COM0000392(EN)/COM0000393(FR)**. See *Debates*, Vo. 151, No 330 at 16:25-17:35 for third reading debate on Bill C-70.

[49] Vote No 814, House of Commons, 44th Parliament, 1st Session, *Journals*, No 331 (June 13, 2024), **COM0000394**.

[50] *Debates of the Senate*, 1st Session, 44th Parliament, Vol 153, No 208 (June 5, 2024), **COM0000434(EN)/COM0000435(FR)**.

[51] Witnesses listed in the Standing Senate Committee on National Security, Defence and Veterans Affairs Meeting Details for Meeting 56 (June 10, 2024),

[81] On 13 June 2024, Bill C-70 completed first reading in the Senate.[52]

[82] On 17 June 2024, Bill C-70 completed second reading in the Senate.[53]

[83] On 18 June 2024, SECD completed its clause-by-clause review.[54] The Committee reported Bill C-70 to the Senate without amendment. However, SECD made the following observations:

> Your committee recognizes that the Royal Canadian Mounted Police (RCMP) does not have sufficient resources to address the additional burden on criminal investigation and enforcement that this bill would create. The Government of Canada must ensure that the quantity and quality of national policing resources is adequate for a rapid and comprehensive response by the RCMP to an ever-changing threat environment.
>
> Your committee heard that Canadian universities are concerned that their partnerships with foreign universities that might be publicly funded could be put at risk by the proposed Foreign Influence Transparency Registry, and that it could put a chilling effect on international collaboration and exchange in the academic community. It is crucial that the Government of Canada appoint a Foreign Influence Transparency Commissioner as soon as possible, and that upon their appointment the Commissioner engage in constructive, mutually beneficial dialogue with universities, including by communicating proactively with them, so they understand — and are aware of — their obligations under the proposed registry.
>
> Your committee recognizes that concerns have been raised about potential unintended impacts on diaspora communities and on individual rights, including freedom of expression and freedom of association.
>
> Given the importance of the subject matter of Bill C-70, the committee is of the opinion that it would have benefitted from additional time to study this legislation.[55]

COM0000407(EN)/COM0000411(FR); Meeting 57 (June 12, 2024), **COM0000408(EN)/COM0000412(FR)**; Meeting 58 (June 13, 2024), **COM0000409(EN)/COM0000413(FR)**.

[52] *Debates of the Senate*, 1st Session, 44th Parliament, Vol 153, No 212 (June 13, 2024), **COM0000436(EN)/COM0000437(FR)**.

[53] *Debates of the Senate*, 1st Session, 44th Parliament, Vol 153, No 213 (June 17, 2024), **COM0000438(EN)/COM0000439(FR)**.

[54] Standing Senate Committee on National Security, Defence and Veterans Affairs, Meeting 59 (June 18, 2024), **COM0000410(EN)/COM0000414(FR)**.

[55] Report of the Standing Senate Committee National Security, Defence and Veterans Affairs, Tenth Report (June 18, 2024), **COM0000416(EN)/COM0000415(FR)**.

[84] On 19 June 2024, Bill C-70 completed third reading in the Senate.[56]

[85] On 20 June 2024, Bill C-70 received Royal Assent. The amendments to the *CSIS Act* came into effect on that day. Amendments to *SOIA* (now *FISOIA*), the *Criminal Code* and the *Canada Evidence Act* will (with minor exceptions) came into force on 19 August 2024 (60 days after Royal Assent). *FITAA* will come into force on a day fixed by order in council. Public Safety estimates the Foreign Influence Transparency Registry will take a year to set up.[57]

[56] *Debates of the Senate*, 44th Parliament, 1st Session, Vol 153, No 215 (June 19, 2024), **COM0000440(EN)/COM0000441(FR)**.

[57] *An Act respecting countering foreign interference*, S.C. 2024, c. 16, **COM0000381**.