LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

LEGISLATIVE SUMMARY

Bill C-22:

An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts

Publication No. 42-1-C22-E
22 August 2016

Holly Porteous
Dominique Valiquet

Legal and Social Affairs Division
Parliamentary Information and Research Service

Library of Parliament ***Legislative Summaries*** summarize government bills currently before Parliament and provide background about them in an objective and impartial manner. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations. Legislative Summaries are revised as needed to reflect amendments made to bills as they move through the legislative process.

Notice: For clarity of exposition, the legislative proposals set out in the bill described in this Legislative Summary are stated as if they had already been adopted or were in force. It is important to note, however, that bills may be amended during their consideration by the House of Commons and Senate, and have no force or effect unless and until they are passed by both houses of Parliament, receive Royal Assent, and come into force.

Any substantive changes in this Legislative Summary that have been made since the preceding issue are indicated in **bold print**.

Legislative Summary of Bill C-22
(Legislative Summary)

Publication No. 42-1-C22-E

Ce document est également publié en français.

CONTENTS

LEGISLATIVE SUMMARY OF BILL C-22: AN ACT TO ESTABLISH THE NATIONAL SECURITY AND INTELLIGENCE COMMITTEE OF PARLIAMENTARIANS AND TO MAKE CONSEQUENTIAL AMENDMENTS TO CERTAIN ACTS

1 BACKGROUND

Bill C-22, An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts[1] was introduced in the House of Commons on 16 June 2016.

Bill C-22 aims to deliver on an election pledge of the current government to more closely align Canada's national security accountability regime with those of its Five Eyes allies (the United States, the United Kingdom, Australia and New Zealand) by creating "an all-party committee to monitor and oversee the operations of every government department and agency with national security responsibilities."[2]

During planning for the bill, the Minister of Public Safety and Emergency Preparedness, the Honourable Ralph Goodale, and the presumed Chair of the National Security and Intelligence Committee of Parliamentarians (NSICOP), David McGuinty, MP,[3] held discussions in France, New Zealand, the United Kingdom and the United States to examine these countries' respective legislative oversight committees.[4] It appears that the Canadian delegation saw the British model as the most appropriate template for the NSICOP.[5]

Though Bill C-22 incorporates many features of the United Kingdom's Intelligence and Security Committee (ISC), it also deviates from this model in significant ways and does not fully match the ISC as it has evolved over time. Indeed, the proposed NSICOP most closely resembles the ISC, not as this committee is currently constituted, but rather as it existed prior to reforms made under the United Kingdom's *Justice and Security Act 2013*.[6]

Given the apparent influence of the British model on Bill C-22, the following sections will provide a high-level comparison between the two approaches.

2 DESCRIPTION AND ANALYSIS

Bill C-22 contains 49 clauses. The following description highlights certain aspects of the bill; it does not review every clause.

2.1 Committee and Members (Clauses 4 to 7 and 12)

Bill C-22 establishes a nine-member committee of parliamentarians (including the chair), housed in the executive branch and appointed by and reporting to the prime minister. The committee comprises up to two senators and not more than seven members of the House of Commons, including as many as four from the governing party. Acting on the recommendation of the prime minister, the Governor in Council designates the chair from among the members of the committee. Serving ministers and parliamentary secretaries are not eligible for membership in the NSICOP.

Members of the House of Commons from the non-governing parties with a recognized membership of 12 or more persons in the House of Commons may be appointed only after the prime minister has consulted the leaders of their respective parties. Similarly, the prime minister is obliged to consult one or more senators prior to appointing the Senate members of the committee.

Under clause 5(1), all committee members lose their positions upon dissolution of Parliament. There is no provision for reappointment to the committee.

Clause 12(1) removes the ability of NSICOP members, past and present, to claim parliamentary privilege in any proceeding undertaken against them for unauthorized disclosure of protected information accessed in the course of their NSICOP work.

In the absence of clause 12(2), clause 12(1) would be redundant. Clause 12(2) establishes that a statement made by a member or former member of the committee before either House of Parliament or a committee of the Senate, of the House of Commons or of both Houses of Parliament is admissible in evidence against him or her in a court proceeding concerning a contravention of the *Security of Information Act*.

Parliamentary privilege does not apply to non-parliamentary proceedings, such as those held by the NSICOP. However, the work of NSICOP members will be part-time and these parliamentarians are still expected to conduct their regular parliamentary duties, presumably including committee work. Thus, clause 12(2) prevents the application of parliamentary privilege to statements made by current and past NSICOP members in either the House of Commons or Senate that result in the unauthorized disclosure of protected information.

2.1.1 Comparison with the United Kingdom

At one time, the British approach to establishing membership of its review committee, the ISC, was less consultative than that set out in Bill C-22. Prior to the enactment of the *Justice and Security Act 2013* – which replaced the ISC's enabling legislation, the *Intelligence Services Act 1994*[7] – the British prime minister directly appointed members to the ISC. Now, the prime minister consults the leader of the opposition prior to nominating members. Each of the members nominated by the prime minister is then either appointed or rejected by the House of Parliament from which he or she is drawn.

The ISC's membership – like that of the NSICOP – is dominated by the House of Commons. Since its inception, the ISC has never had as members more than two peers from the House of Lords at any one time. However, unlike the NSICOP, the ISC is chaired by a person chosen by its members.

As stipulated for members of the NSICOP, ISC members lose their memberships upon dissolution of Parliament, although, unlike Bill C-22, reappointment is possible.[8] Sections 1(6) and 1(7) of Schedule 1 of the *Justice and Security Act 2013* provide for continuity of the ISC's work by permitting work in progress or actions taken to be carried over into the next parliament. It is not clear how continuity of the NSICOP's work and actions from one parliament to the next is provided for in Bill C-22.

Pursuant to the *Justice and Security Act 2013*, the status of the ISC changed from a committee of parliamentarians to a parliamentary committee. In proposing a committee of parliamentarians, Bill C-22 constitutes the NSICOP as an administrative body separate from Parliament. This means that the NSICOP is accountable to the prime minister alone.

Of note, the *Justice and Security Act 2013* does not remove parliamentary privilege from ISC members.

2.2 Mandate (Clauses 8, 9 and 31)

Under clause 8, the NSICOP is mandated to review:

> (a) the legislative, regulatory, policy, administrative and financial framework for national security and intelligence;
>
> (b) any activity carried out by a department that relates to national security or intelligence, unless the appropriate Minister determines that the review would be injurious to national security; and
>
> (c) any matter relating to national security or intelligence that a minister of the Crown refers to the Committee.

2.2.1 Review of Ongoing Operations

In a backgrounder released when Bill C-22 was tabled, the government said that the "NSICOP would be empowered to perform reviews of national security and intelligence activities including *ongoing operations*." [Authors' emphasis][9] A possible explanation of how an *ex post* (after-the-fact) review model can be said to provide for examination of ongoing operations might be found in how the Communications Security Establishment (CSE) Commissioner and Security Intelligence Review Committee (SIRC) execute their respective mandates.

For example, section 273.63(2)(a) of the *National Defence Act*[10] mandates the CSE Commissioner "to review the activities of the Establishment to ensure that they are in compliance with the law." A collection of annually renewed ministerial authorizations are a key element in how CSE conducts itself lawfully. These ministerial authorizations shield CSE from liability under Part VI of the *Criminal Code*[11] arising from the interception of private communications in the course of conducting mandated foreign intelligence and cyber protection activities. In effect, the Minister of National Defence authorizes CSE to engage in activities where there is a risk of the law being

broken, but places conditions on how it undertakes these activities so that the privacy of Canadians is protected to the greatest extent possible. Some of these activities, it should be noted, could be considered ongoing operations, as they carry on uninterrupted as one authorization expires and its replacement immediately comes into effect.

Once a ministerial authorization expires, the CSE Commissioner executes his or her mandate by reviewing whether CSE activities conformed to all aspects of the authorization, including conditions imposed by the Minister of National Defence. If there are issues to be addressed, the CSE Commissioner can recommend changes before CSE requests renewed authorization. In fact, an authorization can be changed or cancelled at any point.

A roughly similar dynamic can also take place when SIRC reviews Canadian Security Intelligence Service (CSIS) investigations carried out under warrants.[12] Federal Court judges, from whom CSIS obtains warrants, can also query the service on its implementation of the Court's orders. Thus, an *ex post* review could also be considered a review of an ongoing operation.

2.2.1.1 Comparison with the United Kingdom

The question of operational review has unfolded differently in the United Kingdom. There, the *Justice and Security Act 2013* amended the ISC's existing mandate to make explicit reference to operations. However, neither this Act nor the Investigatory Powers Bill[13] defines what is meant by "operation." According to the 2011–2012 annual report of the ISC, the committee had been examining operational issues since at least 1999, and it felt that a change in its mandate would simply formalize the existing reality.[14] Nonetheless, it seems that the ISC wanted the statutory change because it was encountering difficulties in accessing information. Essentially, the intelligence agencies were pushing back against ISC efforts to obtain information the committee believed it needed to hold the government accountable.[15]

Though the ISC is now mandated to examine matters related to operations, it still faces certain limitations on its remit in this area. At present, the ISC may examine an operational matter only if both the committee and the prime minister are satisfied that the matter is not part of any ongoing intelligence or security operation and it is of significant national interest.[16]

Furthermore, the *Justice and Security Act 2013* permits the ISC to review operational matters only on the basis of information that has been voluntarily provided to it by the intelligence agencies or relevant government departments, thus effectively prohibiting receipt of information from government whistleblowers. The potential impact of Bill C-22's provisions on the NSICOP's receipt of information from whistleblowers or pertaining to them will be discussed in section 2.3.1 of this Legislative Summary.

Finally, the *Justice and Security Act 2013* requires the ISC to conduct reviews of operational matters in a manner consistent with a memorandum of understanding (MOU) agreed to by the ISC and the prime minister and tabled in Parliament as part of the ISC's 2013–2014 annual report.[17] This MOU enables the ISC, with government approval, to adjust its scope of review to reflect changes in the structure and work of the intelligence community.[18]

2.2.2 Ministerial Discretion

As outlined above, clause 8(b) allows the NSICOP to review any activity carried out by a department that relates to national security or intelligence, unless the appropriate minister determines that the review would be injurious to national security. This clause introduces a potentially significant limitation on the committee's remit. The determination of what might be injurious is left entirely to the minister, as is made clear in clause 31(1), which states that the minister's decisions on proposed reviews and on refusals to provide information are final. It would appear that the committee is not consulted, as happens in the United Kingdom when the ISC proposes a review of an operational matter.

Moreover, the minister is not obliged to justify his or her decision to the NSICOP, and Bill C-22 does not provide for judicial review. As indicated in clause 31(2), the NSICOP can do no more than express its dissatisfaction in an annual or special report to the prime minister. In addition, the public may never be made aware that an NSICOP-initiated review was quashed. After consulting the NSICOP chair, the prime minister can direct that the NSICOP's expression of dissatisfaction be removed from the version of the report that is tabled in Parliament on the grounds that it is injurious to national security, national defence or international relations, or that the information contained in the expression of dissatisfaction is protected by a legal immunity such as solicitor–client privilege. Once again, the NSICOP has no avenue for appeal of such a directive.

2.2.3 Unnecessary Duplication of Work

Clause 8(c) of Bill C-22 reflects the British model, in that it envisions executive branch requests for the examination of specific issues related to national security and intelligence. However, whereas the United Kingdom legislation permits the prime minister alone to make such requests, Bill C-22 stipulates that they are to be made by ministers of relevant departments and agencies.

Clause 9 limits the NSICOP's scope of review, stating that the committee and each review body must "take all reasonable steps to cooperate with each other to avoid any unnecessary duplication of work." However, taking as a guide the list of 17 departments and agencies in Schedule 3 of the *Security of Canada Information Sharing Act*, it appears that the range of sources and issues for such Crown-requested studies could be quite broad and the potential for duplication correspondingly high.[19] It is unclear who will determine whether a proposed review is unnecessarily duplicative.

2.2.3.1 Comparison with the United Kingdom

Similar language regarding duplication of work appears in the MOU between the British prime minister and the ISC.[20] Nevertheless, when the *Justice and Security Act 2013* was enacted, the lawfulness review mandate of the Intelligence Services Commissioner – one of the independent review bodies that focuses on intelligence and national security activities – was broadened to include reviewing "the implementation or effectiveness of particular policies" of the intelligence services.[21] The ISC had opposed this idea on the grounds that adding an efficacy review function to the commissioner's remit would blur lines of authority and cause confusion.[22] Regardless, the ISC's protests failed to stop the change to the Intelligence Services Commissioner's mandate.

Three years on, the British government is now seeking to eliminate the Intelligence Services Commissioner under the Investigatory Powers Bill. If enacted, the bill will replace the Intelligence Services Commissioner, the Interception of Communications Commissioner and the Surveillance Commissioner with a single entity: the Investigatory Powers Commissioner (who would be supported by other judicial commissioners appointed by the prime minister).

While the main function of the proposed Investigatory Powers Commissioner would be to review the issuance and implementation of warrants under this regime – in other words, lawfulness – the bill would also direct the commissioner to keep under review the "carrying out of any aspect of the functions" of an intelligence service, the head of an intelligence service, or any part of the armed forces or Ministry of Defence engaged in intelligence activities.[23] This language could be interpreted to include efficacy review, thus raising once more the possibility of conflict with the ISC's work.

2.3 Security Measures (Clauses 10 to 12 and 33)

Clause 10 requires NSICOP members to undergo and maintain security clearances; to undertake an oath or affirmation of secrecy (included in the schedule of this bill); to be notified that they are permanently bound to secrecy under section 10 of the *Security of Information Act*; and to adhere to security measures promulgated in regulations established by the Governor in Council under clause 33.

Clause 33 indicates that the Governor in Council may promulgate regulations concerning the secure handling, storage, transmission and disposal of information or documents provided to or created by the NSICOP. However, it is not clear if these or other regulations concerning procedural and administrative aspects of the NSICOP's work and referenced in clause 33 will be made public.

Clause 11 further reinforces the obligation of NSICOP members and secretariat staff, both past and present, to maintain secrecy about information to which they have had access or obtained as a result of their work for the committee. Disclosures of information that the government is taking measures to safeguard will be permitted only for the purpose of the NSICOP exercising its powers or performing its duties or functions under this Act or as required by any other law. In this regard, it should be noted that section 15 of the *Security of Information Act* provides for a public interest claim for unauthorized disclosure.

2.3.1 Whistleblowers

There are no specific provisions in Bill C-22 for the NSICOP to receive information from whistleblowers as part of its mandate. Because its members are bound by both the Oath or Solemn Affirmation (included in the schedule to Bill C-22) and the *Security of Information Act*, the NSICOP is prohibited from receiving information directly from government whistleblowers. In particular, the Act prohibits unauthorized communication and receipt of any "secret official code word, password, sketch, plan, model, article, note, document or information."[24]

There is, however, a possibility of obtaining whistleblower information indirectly from bodies that are permitted to receive such information. These bodies include the CSE Commissioner and SIRC, which, under section 15(5) of the *Security of Information Act*, are authorized to receive disclosures about "wrongdoing," including disclosures involving special operational information.[25]

Clause 9 provides for cooperative work between the NSICOP and expert review bodies. It is therefore conceivable that the committee could examine issues raised in a whistleblower complaint that has been investigated by SIRC or the CSE Commissioner. Nonetheless, under clause 8(b), the minister can halt the proposed review on the grounds that it is injurious to national security. Moreover, clause 16(a) enables the minister to refuse to provide information that constitutes special operational information, thus providing another means to prevent NSICOP reviews based on whistleblower disclosures.

2.4 Access to Information (Clauses 13 to 16)

Clause 13(1) establishes the NSICOP's right of access to any information that is under the control of a department or agency and related to the committee's mandate. Significantly, information that foreign intelligence partners share with a Canadian department or agency is not considered to be under the control of that department or agency; rather, it is deemed to be in its possession. Control always lies with the originating entity, which, in this case, is the foreign intelligence partner.[26]

Clause 13(2) confirms that the NSICOP's right of access extends to information that would otherwise be protected by various forms of legal immunity, including information that is subject to solicitor–client privilege.

Clauses 14 to 16 place restrictions on the NSICOP's access to information.

Clause 14 sets out the following list of automatic exceptions:

- Cabinet confidences;
- information pertaining to ongoing defence intelligence activities supporting military operations, including the nature and content of plans in support of those military operations;
- information pertaining to protected persons – and techniques and infrastructures used to protect them – under the Witness Protection Program;
- information about the identities of confidential sources of Canada or its allies;
- information relating directly to an ongoing investigation carried out by a law enforcement agency that may lead to a prosecution;
- information that is privileged under section 36(1) of the *Investment Canada Act*;[27] and
- information that the Financial Transactions and Reports Analysis Centre (FINTRAC) has received but not reported to a department.

On this last point, it is unclear whether the NSICOP can request descriptive information about these FINTRAC holdings, such as the number of reports that have been received but not disclosed.[28]

Clause 15(2) stipulates that requests for information that FINTRAC has disclosed to a department must be directed to the minister responsible for that department. Unless the NSICOP is permitted to request that FINTRAC provide a list of what it has disclosed to departments, this could create difficulties for the committee, as it would force it to approach various ministers who may or may not have received FINTRAC information.

Clause 14 prevents access to information pertaining to ongoing defence intelligence activities that support military operations, effectively eliminating NSICOP review of a broad range of Canadian Forces' current and potential intelligence activities. Indeed, the Canadian Forces Intelligence Command is the only entity within the Canadian intelligence and national security community that conducts every form of intelligence collection – signals intelligence,[29] human intelligence and open-source intelligence.[30]

At present, defence intelligence activities are not subject to any form of independent review.

Clause 16(1) of Bill C-22 authorizes the minister to refuse to provide information to which the NSICOP is otherwise entitled and that is under the control of his or her department. However, the minister is only permitted to do so if he or she believes that the information constitutes special operational information, as defined in section 8(1) of the *Security of Information Act*, and its provision would be injurious to national security.[31]

Clause 16(2) requires the minister refusing access to information under clause 16(1) to inform and provide reasons for decision to the NSICOP. Clause 16(3) requires the minister to inform and provide reasons to a relevant expert review body. Depending on which agency has control of the information, the expert review body will be SIRC, the CSE Commissioner or the Civilian Review and Complaints Commission for the RCMP (CRCC).

Given that none of the review bodies has the authority to challenge the minister's decision, information provided under clause 16(3) essentially serves notice that the review bodies are also barred from sharing this information with the NSICOP. This interpretation is borne out by clause 22(2)(b), which prohibits the review bodies from providing information that is the subject of a clause 16(3) notification.

2.4.1 Comparison with the United Kingdom

The ISC has examined defence intelligence activities for many years. In its 2013 MOU with the prime minister, the ISC describes its remit with respect to the Ministry of Defence as including:

- the strategic intelligence activities undertaken by the Chief of Defence Intelligence, including intelligence collection, analysis and training; and
- offensive cyber.[32]

2.5 Meetings (Clauses 17 to 20)

Bill C-22 does not stipulate how often NSICOP meetings will be held, stating only that they occur when the chair determines them to be necessary.

Clause 18 indicates that meetings should be held privately if information a department is protecting "is likely" to be disclosed or if the chair deems a private meeting necessary.

Under clause 20, the NSICOP is empowered to work out its own procedures in relation to the exercise of any of its powers or the performance of any of its duties or functions, including in respect of the appearance of persons before the committee.

2.5.1 Comparison with the United Kingdom

In an attempt to enhance its credibility with the public, the ISC began to hold some open hearings with security and intelligence officials in 2013.[33] Nonetheless, its meetings are mainly held in secret.

The ISC meets at least once a week. In its most recent annual report, the ISC stated that it had held 17 formal evidence sessions, five formal committee meetings, and "23 other meetings" between September 2015 and June 2016. It indicated that it would have held an eighteenth evidence session, but for the failure of the National Security Secretariat, the Joint Intelligence Secretariat and the Office for Security and Counter-Terrorism to provide requested information prior to the session.[34]

2.6 Review Bodies (Clauses 22 and 23)

Clauses 22 and 23 provide for the sharing of information – subject to certain exceptions – between the NSICOP and the CSE Commissioner, SIRC and the CRCC. Of note, other expert review bodies that regularly examine departments and agencies of the intelligence and national security community, such as the offices of the Privacy Commissioner, the Information Commissioner and the Auditor General, have been excluded from these information-sharing provisions. Both the Privacy Commissioner and the Information Commissioner have jurisdiction to review the adherence of federal departments and agencies, including CSE, CSIS and the RCMP, to the *Privacy Act* and to the *Access to Information Act*. The Auditor General's public reviews of individual and community-wide intelligence and national security undertakings provide valuable insight into how well departments and agencies are managing programs and activities. All three review bodies work at the classified level and all three are officers of Parliament.

In addition, Bill C-22 does not provide for the possibility of dedicated expert review bodies established in the future, such as a review body for the Canada Border Services Agency.

2.6.1 Comparison with the United Kingdom

The *Justice and Security Act 2013* does not enable the ISC to access classified information from expert review bodies, such as the Intelligence Services Commissioner.

In its 2010–2011 annual report, the ISC said that it had been trying since 2002 to obtain access to classified annexes of Intelligence Services Commissioner and Interception of Communications Commissioner reports to the prime minister. While both commissioners told the ISC that they had no objections to sharing this information, the issue was left to the national security advisor to decide.[35] There has been no indication since to suggest that the ISC was ever granted access to this information.

What is more, the draft Investigatory Powers Bill currently under review in Parliament does not provide for information sharing between the ISC and the proposed single independent review body, the Investigatory Powers Commissioner.

2.7 Reports (Clause 21)

Clause 21(1) requires the NSICOP to prepare an annual report for the prime minister on the reviews it conducted, including findings and recommendations. If the NSICOP uses its powers under clause 21(2) to prepare a special report, it must also include a summary of this report in its annual report to the prime minister.

In addition, clause 21(2) empowers the NSICOP to draft special reports on any issue related to its mandate and to submit these reports to the prime minister and appropriate minister at any time. However, clause 21(3) requires the NSICOP, when submitting a special report, to notify the prime minister if it intends to draft a summary of the special report.

Clause 21(5) permits the prime minister, after consultation with the NSICOP chair, to direct that annual or special reports be revised to remove any information he or she believes would be injurious to national security, national defence or international relations if it were disclosed publicly. This directive also applies to information that is protected by litigation privilege or solicitor–client privilege or, in the case of civil law, by immunity from disclosure or the professional secrecy of advocates and notaries.

If the prime minister has received a clause 21(3) notification about the preparation of a special report summary, and the special report itself will not be tabled in Parliament, then clause 21(5) does not apply.

The prime minister must table copies of NSICOP reports – other than special reports that are not being tabled in Parliament – before each House of Parliament on any of the first 45 days on which that House sits after a report is submitted or, if the NSICOP was directed to produce a revised version, after a revised copy is submitted.

No provision in Bill C-22 explicitly enables the NSICOP to let the public know whether information has been redacted from its declassified reports.

2.7.1 Comparison with the United Kingdom

Under section 3(6) of the *Justice and Security Act 2013*, the ISC must table all reports it drafts in Parliament. Though the ISC must submit its annual and special reports to the prime minister for consultation and review prior to tabling, it uses asterisks in the final report to identify any redactions that have been made on national security grounds. In accordance with section 3(5), the ISC also incorporates a statement in its parliamentary reports with respect to these required exclusions.

2.8 Secretariat and Budget (Clauses 24 to 30, 32 and 43)

2.8.1 Secretariat

Clauses 24 to 30 provide for a secretariat, headed by an executive director and headquartered in the National Capital Region, to support the NSICOP's work. The executive director is appointed by the Governor in Council and has the same rank and authorities as a deputy head. The period of his or her appointment is for a term of up to five years, during pleasure, with a possibility of two reappointments.

Clause 28 provides the executive director with authorities to serve as the chief executive officer of the secretariat, meaning that he or she controls and manages this body and all matters connected to it. According to clause 29, this control extends to contracting and entering into memoranda of understanding or other arrangements to engage persons with legal, professional, technical or specialized expertise to advise and assist the NSICOP or any of its members.

Clause 26 provides for a 90-day appointment of an acting executive director if the executive director is incapacitated. The temporary appointment would be made by a privy councillor who, under clause 3, has been designated to serve as a minister for the purposes of the Act. Any appointment longer than 90 days must be approved by the Governor in Council.

Under clause 27, the executive director's remuneration and the reimbursement of travel and living expenses associated with secretariat work are set by the Governor in Council.

Clause 27(2) indicates that the executive director is deemed a public servant employed in the federal public administration and therefore compensated in accordance with the *Public Service Superannuation Act*, the *Government Employees Compensation Act* and any regulations made under section 9 of the *Aeronautics Act*.[36]

Clause 30 states that employees of the secretariat are to be appointed in accordance with the *Public Service Employment Act*.[37] This Act provides a number of options by which appointment can take place, including the deployment or secondment of persons already employed in the public service.

2.8.1.1 Comparison with the United Kingdom

The British situation is similar, in that the ISC's secretariat, along with one part-time investigator, is both managed and staffed by members of the British civil service, on secondment or assignment. By convention – not explicit policy – these assignments and secondments are not made from that country's intelligence agencies.[38]

2.8.2 Budget

Bill C-22 includes a Royal Recommendation, which establishes that the legislation is expected to entail an expenditure of public funds. Requests for funding of government services and programs from the Consolidated Revenue Fund are made through a supply bill.

Since clause 21 requires the NSICOP to report to the prime minister, it is presumably the prime minister's "department" – the Privy Council Office – that would be responsible for appropriating funds through a supply bill to cover the operating expenses of the committee and its secretariat.

Clause 32 provides for the reimbursement of reasonable travel and living expenses incurred as a result of appearing as a witness before the committee.

Clause 43 provides for an annual allowance of $42,000 for the NSICOP chair and $11,900 for committee members in addition to their existing remuneration as parliamentarians.

2.9 Consequential Amendments (Clauses 35 to 48)

Clauses 35 to 48 make consequential amendments to existing legislation. Of particular interest are clauses 35 and 45, which amend the *Access to Information Act*[39] and the *Privacy Act*[40] to prohibit the NSICOP from disclosing any documentation it has obtained or created in the course of fulfilling its mandate. Given that all of the intelligence agencies are subject to both Acts, it is unclear why the NSICOP would be placed outside this legal framework.

2.10 Parliamentary Review and Coming into Force (Clauses 34 and 49)

Clause 34 provides for a review of this Act, five years after its enactment. The review is to be conducted by both the Senate and the House of Commons.

Under clause 49, the coming into force of Bill C-22 will be fixed by an order of the Governor in Council.

NOTES

1. Bill C-22: An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts, 1st Session, 42nd Parliament.

2. Liberal Party of Canada, *Real Change: A New Plan for a Strong Middle Class*, 2015, pp. 31–32. See also Government of Canada, "National Security and Intelligence Committee of Parliamentarians," Backgrounder.

3. On 8 January 2016, Prime Minister Trudeau announced that David McGuinty, MP, would take a leadership role in the National Security and Intelligence Committee of Parliamentarians [NSICOP]. However, no Order in Council can be passed designating him as chair until Bill C-22 is enacted. For the announcement, see Prime Minister of Canada, "Prime Minister of Canada announces new leadership role for MP McGuinty," News release, 8 January 2016.

4. Amanda Connolly, "Goodale, McGuinty head to U.K., France to talk counterterrorism, Parliamentary committee," *iPolitics*, 8 January 2016.

5. Jim Bronskill, "Canada looking to British model for national security committee: Goodale," *The Globe and Mail*, 8 January 2016.

6. United Kingdom, *Justice and Security Act 2013*.

7. United Kingdom, *Intelligence Services Act 1994*.

8. United Kingdom, *Justice and Security Act 2013*, Schedule 1, ss. 1(1) and 1(4).

9. Government of Canada, "National Security and Intelligence Committee of Parliamentarians."

10. *National Defence Act*, R.S.C. 1985, c. N-5.

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

12. Indeed, to understand the profound impact on ongoing operations that a review body can have, one need only note Justice Richard Mosley's reference in *X (Re)* to the role that the public annual reports of the Communications Security Establishment [CSE] Commissioner and Security Intelligence Review Committee [SIRC] played in his decision to revoke a type of warrant that CSIS has been using to investigate Canadians abroad. See *X (Re)*, 2013 FC 1275.

13. United Kingdom, Investigatory Powers Bill 2015–16 to 2016–17. The bill was introduced in the House of Commons on 1 March 2016 and is now at committee stage in the House of Commons and reporting stage in the House of Lords.

14. United Kingdom, Intelligence and Security Committee [ISC], *Annual Report 2011–2012*, p. 51.

15. Prior to 2013, the United Kingdom intelligence agencies, along with the responsible secretary of state, were empowered to veto ISC requests for access to information. According to the ISC's 2007–2008 annual report, "in practice the Committee has been afforded access to highly sensitive and operational information and there has been only one instance where the Committee has been denied sight of specific documents." The report took note that the prime minister had given specific directives to the intelligence agencies to provide the ISC with "access to all of the material necessary" to undertake its review of the 7 July 2005 terrorist attacks on London. It appears, however, that some agencies still held back key information. In its annual report for 2010–2011, the ISC highlighted significant discrepancies between information provided by the British security services to the committee on this issue and that provided to the coroner's inquest. See ISC, *Annual Report 2007–2008*, p. 5; and *Annual Report 2010–2011*, pp. 68–69.

16. Section 2(3) of the *Justice and Security Act 2013* sets out a third possibility: namely, that the ISC studies an issue based on operational information provided voluntarily by the intelligence agencies or departments under the ISC remit. However, this is likely to happen only when the government has deemed such sharing to be in the public interest.

17. United Kingdom, ISC, "Annex A: A Memorandum of Understanding Agreed Between the Prime Minister and the Intelligence and Security Committee of Parliament (ISC)," in *Annual Report 2013–2014*, p. 11.

18. Joanna Dawson, "The Intelligence and Security Committee," *Briefing Paper No. 02178*, United Kingdom House of Commons Library, 2 February 2016, p. 6.

19. *Security of Canada Information Sharing Act*, S.C. 2015, c. 20, s. 2. It should be noted that clause 14 of Bill C-22 automatically excludes review of the Financial Transactions and Reports Analysis Centre [FINTRAC] and most defence intelligence activities.

20. United Kingdom, ISC, "Annex A," in *Annual Report 2013–2014*, p. 12.

21. United Kingdom, *Justice and Security Act 2013*, s. 5(4).

22. It seems that the ISC viewed the mandate enlargement as an additional means for the government to deny the committee access to operational information, since the commissioner was already seized with the issue. See United Kingdom, ISC, *Annual Report 2011–2012*, p. 51.

23. United Kingdom, Investigatory Powers Bill, s. 208(1).

24. The *Security of Information Act* also binds those who have been served notice to lifelong secrecy with respect to a highly safeguarded class of information referred to as "special operational information." Clause 41 of Bill C-22 would alter the schedule of the *Security of Information Act* to add the NSICOP to the list of entities whose members or employees are permanently bound to secrecy.

25. The CSE Commissioner and SIRC are permitted to receive and investigate whistleblower disclosures only after the deputy head or Deputy Attorney General has heard the disclosure and failed to respond in a reasonable period of time.

26. This long-standing principle of originator control is explained at length in Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, "Chapter 3.1: Information Sharing – The Original Arrangement," in *Report of the Events Relating to Maher Arar: Factual Background*, Vol. I, 2006, pp. 30–35.

27. *Investment Canada Act*, R.S.C. 1985, c. 28 (1st Supp.).

28. Under FINTRAC's enabling legislation, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17, the organization may disclose information it has received when there are reasonable grounds to suspect money laundering or terrorist activity. However, it appears that FINTRAC receives significantly more reports than it is permitted to disclose. For example, in his 2015 public annual report, FINTRAC's director noted progress made towards destruction of some 17 million reports that had not met the threshold for disclosure but remained within the centre's holdings. See FINTRAC, *Combatting Money Laundering and Terrorism Financing: FINTRAC Annual Report 2015*, p. 4.

29. Signals intelligence includes a number of sub-disciplines: communications intelligence, electronic intelligence and foreign instrumentation signals intelligence.

30. For a high-level description of the organization of Canadian Forces Intelligence Command, see Department of National Defence, *Canadian Forces Intelligence Command*.

31. CSE, CSIS and the RCMP are the only entities designated under the schedule to the *Security of Information Act* that control, rather than simply possess, special operational information. They control this information either because they are its originating source or because they acquired it through a foreign partner and convey all third-party requests to the partner regarding access or use.

32. United Kingdom, ISC, "Annex A," *Annual Report 2013–2014*, p. 12.

33. Unclassified testimony and briefings provided to the ISC are posted online. See United Kingdom, ISC, *Transcripts and Public Evidence*.

34. United Kingdom, ISC, *Annual Report 2015–2016*, p. 7.

35. United Kingdom, ISC, *Annual Report 2010–2011*, p. 84.

36. Section 9 of the *Aeronautics Act* provides compensation for federal employees who suffer death or injury during a flight undertaken in direct connection with their work in the federal public administration. See *Aeronautics Act*, R.S.C. 1985, c. A-2.

37. *Public Service Employment Act*, S.C. 2003, c. 22, ss. 12 and 13.

38. United Kingdom, ISC, *Frequently Asked Questions (FAQs)*.

39. *Access to Information Act*, R.S.C. 1985, c. A-1.

40. *Privacy Act*, R.S.C. 1985, c. P-21.