Explanatory Note on Draft Amendments to the Strategic Services Agency Act proposed by Opposition Senators

Draft Amendments to the Strategic Services Agency Act proposed by Opposition Senators at the 3rd May 2016 sitting of the Senate.

1. Introduction

Opposition Senators propose the **Draft Amendments** (attached) be included as amendments in the Strategic Services Agency (Amendment) Bill, 2016 ("the Bill").

Given the expanded remit of the Strategic Services Agency ("SSA" or "Agency") proposed in the Bill, Opposition Senators are of the view that additional measures are required to monitor and oversee the Agency's activities. The proposed amendments are based on international precedent, recommended best practices and concepts introduced in recent legislation such as the Data Protection Act (Chap. 22:04) ("DPA").

Four types of amendments are proposed:

1) Acceptance of particular amendments already proposed in the Bill;
2) Modification of particular amendments proposed in the Bill;
3) Amendments to existing sections of the parent act, the Strategic Services Agency Act (Chap. 15:06) ("the Act"); and
4) Amendments to add new sections to the Act.

Additionally, Opposition Senators propose consequential amendments to the Interception of Communications Act (Chap. 15:08).

Opposition Senators call for the Bill to be referred to a Joint Select Committee to permit the comprehensive examination of the Bill and the proposed amendments.

2. Objective of Proposed Amendments

The proposed amendments take into account issues which arise from the intended reconfiguration of the SSA into a national intelligence agency.

Abuse of national intelligence powers has occurred in developed nations including, *inter alia* Canada, the United States and the United Kingdom all of which have oversight mechanisms much more intrusive than those that are proposed and/or currently exist in Trinidad & Tobago.

The Act (unchanged by the Bill) provides executive oversight through the Auditor General's scrutiny of the finances of the Agency and legislative oversight through the Annual (operational) Report of the Agency which is laid in Parliament and through the Joint Select Committee on

National Security's ability to question the SSA Director and Agency officials. The Annual Reports of the Auditor General on the SSA for the years 2003 through 2008 and the Annual Reports on the operations of the SSA for the years 2009 through 2013 were all laid in Parliament in 2015. Thus, the value and/or effectiveness of these oversight mechanisms are questionable.

The oversight currently provided is completely *ex post facto* and out of step with modern legislative measures governing intelligence agencies which generally provide for a level of oversight of the day-to-day operations of an intelligence agency. Further, modern legislation generally provides an independent tribunal that has access to the any information in the agency's possession to resolve complaints against the intelligence agency by members of the public and employees of the agency.

The Act (unchanged by the Bill) leaves the day-to-day operations subject to complete executive (thus, political) control. Modern legislation is careful to insulate an intelligence agency's operations from political direction.

Necessary sections of the DPA which regulate the handling and sharing of data to international standards have not yet been proclaimed.

Considering the foregoing, Opposition Senators have prepared Draft Amendments to achieve four primary objectives within the legislation:

1) To appropriately balance privacy rights with national security objectives;

2) To provide mechanisms which reduce the likelihood of abuse of power by the political directorate and/or employees of the Agency;

3) To provide a proportionate level of independent oversight and monitoring of the Agency's activities and to provide an independent tribunal to hear complaints in accordance with international best practices and human rights standards; and

4) To establish safeguards to ensure proper use of intelligence information.

3. Summary of the Proposed Amendments

Upon consideration international precedent, recommended best practices and concepts introduced in recent legislation, Opposition Senators have proposed a number of amendments which narrowly and precisely define the Agency's remit and make sure that the Agency's powers are clearly defined in laws available to the public. (see Practices 2 and 3 in the **Appendix)**

More substantively, the proposed amendments make provision:

- To create a civilian oversight committee independent of both the executive and the legislature is created which may hear complaints from the Agency, employees and the

general public regarding the Agency's activities. The committee is also empowered to conduct investigations of Agency activity and make recommendations. The committee is made up of former Judges and selected in the same manner as the Director and Deputy Directors are proposed to be selected. The civilian oversight committee is granted access to Agency files and may conduct investigations as needed. Whistle-blower protection is created for employees who make a complaint to the oversight committee.

- For the Agency to respect human rights standards adopted by Trinidad and Tobago and to prohibit discriminatory use of intelligence power, such as on the basis of sex, race, ethnicity, religion, political affiliation, gender, etc.

- To insulate the Director and Deputy Director from the political directorate by permitting the appointees to be selected by the President after consultation with the Prime Minister and the Leader of the Opposition, permitting the Salaries Review Commission to set the terms and conditions of appointment, and setting strict provision regarding the removal of the persons serving. The Minister may only issue policy directives to the Agency and the operations of the Agency are to managed by the Director and not mandated by the Minister. To ensure quality candidates minimum educational and professional experience is defined.

- To make the Director, Deputy Director and Intelligence Review Committee members subject to the laws applicable to public officers.

- To create criminal penalties for employees of the Agency and the Intelligence Review Committee for the unauthorised alteration or destruction of intelligence records, for failing to destroy an intelligence record when ordered to do so, and for use of intelligence powers to further or harm the interest of any political or community group (such as members of a religious faith or a non governmental organisation).

- To create provisions related to the management, custody and access to the database that the Agency will maintain and crucial elements of the DPA have not yet been proclaimed and to further, create privacy principles to guide the Agency's management of intelligence data.

- To mandate the signing of intelligence sharing agreements with foreign intelligence agencies so that information is shared (and used) according to written agreements as is required for most international intelligence agencies.

- To require that the Minister pass regulations related to Agency functions, employee grievances and data handling by the Agency.

- To limit Director's powers under the ICA to only be permitted to intercept communications with a warrant, which includes emergency situations.

4. Source of Law and Policy

The primary policy document used in preparing these amendments was *A compilation of good practices on legal and institutional frameworks to ensure respect for human rights by intelligence agencies* published in 2010 for the United Nations General Assembly by the Human Rights Council ("the UN Report"). The UN Report canvasses the laws governing intelligence agencies in many nations and presents the best practices to ensure the proper functioning of an intelligence agency. The practices are listed in the **Appendix**.

A review of the many reports listed in the **References** section demonstrates great consistency in recommendations related to oversight of intelligence agencies.

In drafting the particular provisions, the laws of many nations were reviewed, including *inter alia* the laws of New Zealand, Canada, the United States, the United Kingdom and Australia. Several research papers discussing the laws of France, the Netherlands, Germany, Switzerland, Sweden and many others were also reviewed (see documents listed in the **References** section). The DPA provisions related to the Information Commissioner's powers were studied carefully when drafting the Intelligence Review Committee sections.

5. A Note on Human Rights Protections in Trinidad & Tobago

The Ministry of the Attorney General houses the International Law and Human Rights Unit which fulfills Trinidad and Tobago's human rights reporting obligations on the implementation of five (5) major International Human Rights Conventions including the International Covenant on Civil and Political Rights ("ICCPR").[1]

In order these conventions to receive effect in Trinidad and Tobago, they must either be incorporated into legislation directly or incorporated in legislation through principles, concepts, or particular measures from the convention.

The international trend is to include human rights protections in legislation governing intelligence agency activity.[2] One such protection is found in article 17 of the ICCPR which Trinidad and Tobago is a party to: "no one shall be subjected to arbitrary and unlawful interference with his or her privacy, family, home or correspondence…"[3] See also Article 12 of the UN Universal Declaration of Human Rights

[1] http://www.ag.gov.tt/Features/The-Law-and-You

[2] *Summary of the Human Rights Council panel discussion on the right to privacy in the digital age,* A/HRC/28/39

[3] ICCPR (U.N.) (ratified Dec. 16, 1966) available at http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

During the 68th General Assembly, the United Nations passed Resolution 68/167 calling on states "to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data … with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.".

The Human Rights Council produced several reports on the topic which are cited in the **References** section. One report examined the protections provided by article 17.[4]

6. Notes on the Particulars of the Proposed Amendments

Below is a summary of the proposed changes to the Act numbered as they are in the proposals. When relevant, reference is made to the parent Act and Bill. Citation is made to the UN Report and to other reference material which provide support for the particular proposal.

No changes are proposed to Sections 1, 11, and 12 of the parent Act and Clauses 1, 2 and 5 of the Bill are accepted.

Please refer to **Draft Amendments** for the particulars of each amendment. Note that full citations to referenced documents are contained in the **References** section.

Section 2 of the Amendments and Act, Clause 3 of the Bill

1) The amendments proposed in Clause 3 of the Bill which define the terms: ammunition, firearms, prohibited weapon, trafficking in children and trafficking in persons and remove the definition for drug trafficking are accepted.

2) The proposed definition in Clause 3 of the Bill for "crime prevention" is proposed to be changed from "combating serious crime" to "attempts to reduce and deter serious crime". The Government has indicated that the Agency is to have no operational or law enforcement powers. The word "combating" is not suitable to describe crime prevention because "combat" implies the use of force to achieve a goal. The dictionary definition of crime prevention is proposed instead to remove any ambiguity that might be interpreted to provide the Agency with law enforcement powers. **See Practices 2, 3, 20.**

3) The definition of "serious crime" is proposed to be changed to a listing of specific offences in Schedule 1. Clause 3 of the Bill indicates that "serious crime" "includes offences related to" a variety of crimes. The term "related to" is not defined in the Bill and it is far too vague and ambiguous a concept to define the Agency's remit. Instead, it is proposed that the actual offences that fall under the Agency's remit are listed. The

[4] *The right to privacy in the digital age,* A/HRC/27/37.

Agency's remit must be precisely defined to avoid unintended grants of power. **See Practices 2, 3, 20, 21.**

Further, the listing of specific offences is proposed to be included as a Schedule to the Act which can be changed by Order of the Minister subject to negative resolution of the Parliament, so as to make the Agency's remit adjustable without Act of Parliament. (see Amendment section 30 below).

4) The new definition for "information sharing agreement" relates to agreements entered into by the Agency to share intelligence information with domestic and international law enforcement agencies (referred to as Services in the Act). **See Practices 31, 32.**

   Section 42(g) of the DPA would require that any intelligence information shared by the SSA with a foreign law enforcement body be done pursuant to an information sharing agreement, but it is not yet proclaimed.

   International best practice is to require information sharing agreements to mitigate the risk of: 1) domestic intelligence agencies using less scrupulous international partners to get information they can't access under local laws; 2) that international partners using domestic intelligence carelessly or in a manner which a) may compromise local law enforcement or b) is ethically contrary to the way the local agency would use such information.[5]

   As it is unclear when the relevant provisions of the DPA will be proclaimed, information sharing agreement requirements should form part of the Bill. The proposed definition has been adapted from the DPA. (See Amendment section 16 below).

5) The new definitions proposed for Chairman, Deputy Chairman, Intelligence Review Committee, and Office of the Intelligence Review Committee relate to the newly proposed sections 32 through 57.

<u>Section 3 of the Amendment (new)</u>

6) Section 3 is proposed to make the Agency subject to the State Liability and Proceedings Act (Chap. 8:02) which governs civil proceedings by and against the Government. **See Practice 15.**

   This has the effect of giving the Ministry of the Attorney General the responsibility of defending the Agency's breach of the laws and Constitution of Trinidad and Tobago.

[5] *SIPRI Yearbook 2007: Armaments, Disarmament and International Security, Chap. 5,* Pg 200-1

Further, it ensures funds are available to pay out claims as the Ministry of Finance will be responsible for paying out claims rather than the Agency through Parliament.

Massive liabilities could occur should the Agency's powers be used improperly and there must be funding to settle any liabilities which may occur. Further, the Attorney General is the guardian of the public interest and other proposed amendments (below) require the Agency to report potential misconduct and other matters to the Attorney General. In the circumstances, it is appropriate for the Attorney General to have the responsibility for defending the Agency's actions in civil suits.

Section 4 of the Amendment (new)

7) Section 4 is proposed to remove any ambiguity about whether the Agency has any law enforcement powers. The Government has stated that the Agency in not intended to have any law enforcement powers. **See Practice 20, 27.**

Despite the Government's intention, it is quite possible that certain provisions of the Act could be creatively interpreted to give the Agency implied law enforcement powers most of which are addressed by the proposed amendments. Regardless, the Agency's remit should be precisely defined to prevent unintended grants of power, thus a strict prohibition is introduced.

Section 5 of the Amendment (new)

8) Section 5 is proposed to make the heads of the Agency and the Intelligence Review Committee public officers which will make them subject to the Integrity in Public Life Act (Ch. 22:01) ("IPLA"). Further it means that said individuals are subject to the actions related to public officers, such as misconduct in public office. **See Practice 15.**

The reporting requirements which guard against conflict of interest and financial impropriety as well as the potential liability for acts done as a public officer will serve to guard against the improper or arbitrary use of powers granted under the Act.

Section 6 of the Amendment, Section 3 of the Act

9) Subsection 6(1) of the amendment modifies subsection 3(1) of the Act to include a Deputy Director as part of the formation of the Agency. The Act does not refer to a Deputy Director of the Agency, who is expected to wield significant power. Note the Amendments refer to a single Deputy Director and this may need to be expanded based on the Government's proposal for the structure of the Agency.

10) Subsection 6(2) is proposed to define general principles that the Agency should abide by based on laws of other jurisdictions.

- In Trinidad and Tobago, human rights are protected by the Constitution and the international conventions to which the county is a party but only if the convention is entered into law directly, by incorporation of principles, concepts, or particular measures in the convention. **See Practices 4, 5, 17.** Thus, subparagraph 2(b)(i) incorporates human rights standards.

- In subparagraph 2(b)(iii) the requirement of the Agency to act "independently and impartially" makes it a guiding principle for the Agency to maintain independence from political interference. A fundamental issue in drafting laws for intelligence agencies is finding a suitable method which mandates that the agency maintains a level of independence from the political will. **See Practice 12.**

- International best practices are adopted in subparagraph 2(b)(iii) which indicates that Agency should facilitate oversight, not at the expense of national security but in the manner prescribed by laws. **See Practices 11, 19.**

11) Subsection 3(2) of the Act is removed and the relationship between the Director and Minister is defined in new section 11.

<u>Section 7 of the Amendment (new), Section 4 of the Act</u>

12) Section 7 and 8 are intended to create stability of tenure and to limit political interference in the selection of the Director and Deputy Director. **See Practice 12 which speaks to provisions to maintain director neutrality.**

13) Subsection 7(1) is amends subsection 4(1) of the Act to add the position of Deputy Director as a position appointed by the President. The reappointment and termination clauses are moved to sections below.

14) Subsection 7(2) sets the minimum qualifications for the Director and Deputy Director. The criteria contained in Schedule 2 is based on the 2011 Steering Committee Report recommendation for the head of the National Intelligence Agency.

15) Subsection 7(3) is added to require the President to appoint a Director or Deputy Director after consultation with the Leader of the Opposition and Prime Minister as is done for heads of the Service Commissions and the Commissioner of Police. This measure will insulate the Director from improper influence by a politician.

16) Subsection 7(4) is included to authorise the Salary Review Commission ("SRC") set the terms of appointment and the salary for the Director and Deputy Director in place of

subsection 4(3) of the Act. This will reduce the likelihood of political interference by shifting this power to set terms and conditions of appointment from Cabinet to the SRC.

17) Subsection 7(5) is proposed to make the Director and Deputy Director eligible for reappointment as was previously contained in subsection 4(1) of the Act.

18) Subsection 7(6) amends subsection 4(2) of the Act to allow the temporary appointment of Deputy Director and Director as was provided previously for the Director alone with an amendment to limit the term of service as a temporary appointee to either position for a maximum of 12 months. The purpose is to limit the amount of time whereby a temporary person is appointed and force a full time appointment under 7(3).

19) Subsection 7(7) is proposed to permit the Minister to change the minimum criteria for Director and/or Deputy Director by Order subject to affirmative resolution of Parliament. Affirmative resolution is required so that any rationale to modify the criteria shall receive parliamentary scrutiny.

20) Subsection 4(4) of the Act is moved to new section 11.

21) Subsection 4(5) of the Act is removed and the relationship between the Director and Minister is defined in new section 11.

Section 8 of the Amendment (new)

22) In order to give a stability to the Agency and the individuals serving as Director or Deputy Director the terms of removal are proposed based on the criteria for removal of a Public Service Commissioner and two additional reasons based on international precedent. **See Practice 12.**

Section 9 of the Amendment (new), Section 4(4) of the Act

23) Subsections 9(1) and 9(3) are unmodified subsections 4(4)(a) and (c) of the Act.

24) Subsection 9(2) amends section 4(4)(b) of the Act to require that the Director send his annual report on the operations of the Agency to the Intelligence Review Committee so that the committee can monitor Agency activities.

25) Subsections 9(4) and 9(5) are proposed to require that the Director take steps to make sure the Agency (employees) does not act beyond its remit and does not seek out information that is not necessary to its remit. **See Practices 3, 21.**

26) Subsection 9(6) requires that the Director take steps to apply the General Privacy Principles adapted from the Data Protection Act, s. 6 which are based on principles recommended in the U.N. Report. Currently the General Privacy Principles listed in section 6 of the DPA would apply to the Agency. The DPA needs to be amended to create national security exceptions to the General Privacy Principles as certain principles should not apply to the Agency. **See Practices 3, 21-24.**

Section 10 of the Amendment (new)

27) Subsections 10(1) through 10(3) are proposed to ensure certain items which should be available for parliamentary scrutiny form part of the Agency's report. **See Practice 34.**

Section 11 of the Amendment (new)

28) In keeping with the general policy of promoting the independence of the Agency and to sever the potential for executive interference, the Minister is barred from instructing the operations of the Agency. This would necessarily preclude the Minister from instructing the Director to stop collecting intelligence regarding an individual, to collect intelligence information on a particular individual, to destroy intelligence information, etc. **See Practices 12, 13.**

Section 12 of the Amendment, Section 5 of the Act

29) The only amendment is to update the reference to the Schedule to be consistent with the amendments.

Section 13 of the Amendment (new)

30) Subsection 13(1) mandates that the Agency does not use its power to intentionally harm the interests of any political party or other community groups. This is meant to protect groups such as the religious or trade unions or the media for example. **See Practices 11-13.**

31) Subsection 13(2) creates liability for a person who intentionally misuses the Agency power. Given the past behaviour of spy agencies in Trinidad and Tobago this sort of measure is required. The Opposition welcomes a discussion of the terms of liability. **See Practice 15, 16.**

Section 14 of the Amendment (new)

32) Subsection 14(1) mandates for the Director to report the potential unlawful activity of an employee of the Agency to the Minister.

33) Subsection 14(2) mandates the Minister to further report the potential unlawful activity to the Attorney General, the DPP and the Intelligence Review Committee. For proper oversight it is important that there is transparency to stakeholders of potential violations. The Minister is given the opportunity to comment on a report before it is sent out.

34) This section is based on Canadian law.

Section 15 of the Amendment, Section 6 of the Act

35) Subparagraphs 15(1)(d),(e),(f),(h),(j),(k),(l) and 2(a),(c),(d),(e),(f),(i),(j) from the bill are accepted, though some subparagraphs are renumbered based on the below amendments.

36) Generally, amendments to Section 6 of the Act are made in order to precisely define the remit of the Agency. **See Practices 2, 3, 21.**

37) In Subparagraph 15(1)(a) the phrase "for co-ordinating operations for the suppression of serious crime is removed" because the Government has indicated that the Agency is not to take part in law enforcement operations. Co-ordinating operations would potentially put the Agency at the forefront of a law enforcement operation to suppress serious crime.

38) In Subparagraph 15(1)(b) the phrase "develop strategic intelligence" has been removed as it is vague and unclear.

39) In subparagraph 15(1)(c) the phrase "stimulate action towards" has been removed because this also indicates that the Agency will take an operational role in the execution of a strategy.

40) The Bill amendments to subparagraph 15(1)(g) are rejected because the phrase "sophisticated criminal activity" is overly vague in the use of the term "sophisticated". Further criminal activity is not defined in the Act

41) Subparagraph 15(1)(i) is proposed to be removed because it is unclear what the subparagraph means. Further, it is unclear who the strategic intelligence is being provided to.

42) Subparagraph 15(2)(b) is partially reject as it is unclear what disclosures have to be made under which legislation. This section should refer to the specific laws mandating disclosures to an intelligence agency like the Strategic Service Agency.

43) Subparagraph 15(2)(g) is partially rejected because the term "offences related to serious crime" in (i) and "concerning serious crime" in (ii) are overly broad and not sufficiently

concise to define the Agency's remit. Proposed subparagraph g(ii)(D) is accepted and g(ii)(E) is accepted but renumbered to subparagraph (iii).

44) Subparagraph 15(2)(h) of the Act is removed and moved to Section 17 as other provisions related to the keeping of a database by the Agency must be added.

Section 16 of the Amendment (new)

45) Subsection 16(1) is adapted from the DPA s. 42(g). (see section 2 of amendments) **See Practice 31.**

46) Subsection 16(2) permits the DPA to enter into information sharing agreements with local Services but does not make it mandatory.

47) Subsection 16(3) makes the Minister responsible for approving intelligence sharing agreements and a copy must by provided to the Intelligence Review Committee. **See Practice 32.**

48) Subsection 16(4) ensures that the Intelligence Review Committee is sent a copy of any information sharing agreement applicable to the Agency, so that it may receive appropriate scrutiny. **See Practice 34.**

Section 17 of the Amendment (new)

49) For Sections 17 through 20 **see Practices 21 through 26.**

50) Subsection 1 permits the Agency to maintain a database of persons who have been charged or convicted of a serious crime. The Bill proposed to allow the Agency to maintain a database of persons "involved in serious crime" (at section 6(2)(h) of the Act). This proposal is rejected to due to the lack of definition of the term "involved in" which is too vague of a concept to be used to define this activity. The remit of the Agency must be strictly defined. **See Practice 2, 3, 21.**

51) Subsection 2 maintains the provision currently found in section 6(2)(h) of the Act to preserve activity which has been permitted for the last 20 plus years.

52) The authorisation of the Agency to maintain a database is made subject to new sections 18 through 20.

Section 18 of the Amendment (new)

53) Subsection 1 is based on section 35 of the DPA which is still unproclaimed and would require the Agency to carry out this activity. The Agency should not maintain a database without this provision. **See Practice 23.**

54) Subsection 2 requires that the Agency create a system by which access to intelligence information is recorded in a manner necessary to ensure that the oversight Intelligence Review Committee is effective.

55) Subsection 3 sets the standard that must be met by an international partner before information can be shared based on section 36 of the DPA which is still unproclaimed. **See Practices 33, 35.**

56) Subsection 4 requires that the Agency sets levels of security clearance to access information within the Agency to ensure that the oversight Intelligence Review Committee is effective.

Section 19 of the Amendment (new)

57) Subsection 1 requires that intelligence information which comes into the possession of the Agency which is not necessary for the proper discharge of its functions is destroyed. **See Practice 24, 35.**

58) Subsection 2 makes an employee who is responsible for destroying information under subsection 1 liable for failing to destroy the information. The Opposition is open to a discussion regarding the terms of liability for this offence. **See Practice 15, 16.**

Section 20 of the Amendment (new)

59) This section requires the Agency to keep its records up to date and accurate. **See Practice 24.**

Section 21 of the Amendment (new)

60) Subsections 1-3 are proposed to create offences for the copying, stealing, alteration, unauthorised disclosure and destruction (without authorisation) of intelligence information. Previously only the unauthorised disclosure of information was an offence under section 8(3) of the Act. **See Practice 15, 16.**

Section 22 of the Amendment

61) This section is renumbered from section 7 of the Act

Section 23 of the Amendment

62) This section is renumbered from section 8 of the Act

63) Section 8(3) has been removed from this section and moved to section 21 of the amendments so that it is consolidated with other data related offences

64) Section 23(3) adds a provision to ensure that any unauthorised disclosure is reported to the Intelligence Review Committee so that they can perform their oversight functions properly. **See Practice 18.**

Section 24 of the Amendment, Bill Clause 4

65) This section is renumbered section 9 of the Act. The amendments proposed in the Bill are accepted.

Section 25 of the Amendment

66) This section is renumbered section 10 of the Act.

67) Subsections 10(4) and 10(5) are amended to require the Auditor General to provide his report to the Intelligence Review Committee as well as to inform the committee of any irregularities found during an audit of the Agency.

Section 26/27 of the Amendment

68) These sections are renumbered sections 11 and 12 of the Act.

Section 28 of the Amendment

69) This section is renumbered section 13 of the Act which is amended to require the Minister to lay the report of the Intelligence Review Committee in Parliament

Section 29 of the Amendment

70) This section amends section 14 of the Act to require the Minister to create regulations for the Agency subject to the affirmative resolution of Parliament. The rules regulating employee conduct, Agency functions and data handling procedures should be made available to the public. **See Practices 2 and 3.**

Section 30 of the Amendment (new)

71) This section permits the Minister to change the serious crime offenses which fall under the Agency's remit by Order subject to negative resolution of Parliament.

Section 31 of the Amendment (new)

72) This section permits the Minister to change the General Privacy Principles which the Minister is required to take action ensure by Order subject to negative resolution of Parliament.

Sections 32 through 57 of the Amendment (new)

73) These sections create an independent Intelligence Review Committee ("Committee") which is made up of between three to five judges appointed by the President after consultation with the Prime Minister and the Leader of the Opposition. Many of the sections are similar to the provisions for the Agency, e.g. the provisions regarding appointment and removal, terms and conditions of appointment, secondment, employment of staff and these sections are omitted from discussion below. **See Practices 6, 7, 9, 10, 18, 25, 26, 34.**

Section 36 of the Amendment (new)

74) The Committee has four major functions which are captured in this Section: 1) make recommendations on Agency operations based on its investigations; 2) monitor Agency activities for compliance with the laws of Trinidad and Tobago including receipt and review of various reports the Agency must make to the Committee under the amendments; and 3) hear complaints from members of the public and employees of the Agency regarding Agency activities.

Section 37 of the Amendment (new)

75) This section lays out the activities which may be conducted by the Committee pursuant to the functions listed in section 36 including, the authority to conduct investigations and make orders, appropriate in the circumstances, on determining a complaint filed with the Committee. **See Practices 6, 7, 9.**

Section 38 of the Amendment (new)

76) This section makes the Agency records and information available to the Committee to the extent that the information is needed for the Committee to discharge its duties. **See Practices 7, 10.**

Section 39 of the Amendment (new)

77) This section gives the Committee the power to request the Agency to conduct a review of specific functions of the Agency and create a report or the Committee may conduct the review itself if it would be inappropriate for the Agency to conduct the review.

Section 40 of the Amendment (new)

78) This section gives an individual the right to request the Committee to disclose whether the Agency has collected any information related to the individual and whether the information was collected in accordance with the law. There are exceptions for the national security interest. These provisions are basically the lowest level of access given to members of the public regarding information gathered by an intelligence agency. **See Practice 26.**

Section 41 though 47 of the Amendment (new)

79) These sections lay out the complaint resolution powers of the Committee and is based partially on Canadian law. The Committee has the power to administer oaths and demand information or persons be brought before it. A statement made under oath may only be used in a perjury case or in the prosecution of an offence under this Act. A person may file for judicial review of a decision made by the Committee. At the close of a case a report on the outcome of a complaint shall be sent to the Attorney General, DPP, the Minister and the Director. The Committee's jurisdiction does not include employment matters which are handled by grievance procedures of the Agency or the Service Commissions (in cases of secondment). **See Practices 9, 18.**

Sections 48 of the Amendment (new)

80) This section permits the Minister to meet with the Intelligence Review Committee at least once a year and to request that the Committee to prepare a special report.

Sections 49, 57 of the Amendment (new)

81) These sections require the Committee to send the Minister an Annual Report on Operations for laying in Parliament and requires the Auditor General to audit the finances of the Agency

82) The Committee is to be financed through monies provided by Parliament.

Sections 50-56 of the Amendment (new)

83) These sections lay out a number of offences under the Intelligence Review Committee sections including an offence for an employee or Director of Agency who retaliates against an employee for making a report to the Committee. **See Practice 8, 19.**

CONSEQUENTIAL AMENDMENTS TO OTHER ACTS

1) Amendments are proposed to section 6(2)(b) and 20 of the ICA. These amendments are proposed to remove the SSA Director from the list of authorised officers who may

conduct a warrantless interception of communication. The Director still has recourse to intercept communications through the warrant provisions found at sections 8 and 10 of the ICA. Most countries have protections which prevent intelligence agency's from gathering intelligence on citizens without a warrant and if there is any warrantless interception permitted it is in few circumstances (such as impending terrorist attack). In fact, it is one of the reasons the FBI and CIA are not consolidated into a single agency. **See Practice 20.**

7. Reference Material

Policy Papers and Reports

Parliamentary oversight of the security sector, Office for Promotion of Parliamentary Democracy, European Parliament, European Union (2013) available at http://www.dcaf.ch/content/download/153719/2390045/file/EP_Parliamentary_Oversight_Security_Sector_2013_BOH.pdf

The right to privacy in the digital age, Report of the United Nations Commissioner for Human Rights, A/HRC/27/37, Annual Report of the United Nations High Commissioner for Human Rights and reports of the Officer of the High Commissioner and the Secretary-General, Human Rights Council, Twenty-seventh Session (Jun. 30, 2014) available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Summary of the Human Rights Council panel discussion on the right to privacy in the digital age, A/HRC/28/39, Report of the Office of the United Nations High Commissioner for Human Rights, Human Rights Council, Twenty-seventh Session (Dec. 19, 2014) available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39

Report on the promotion and protection of human rights and fundamental freedoms while countering terrorism - Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, A/HRC/14/46, Schenin, M., Special Rapporteur, Human Rights Council, United Nations (May 17, 2010) available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf

Overseeing Intelligence Services: A Toolkit, Born, H., Wills, A., Geneva Centre for the Democratic Control of Armed Forces (2012) (see Tool 2: Establishing Effective Oversight Systems) available at http://www.dcaf.ch/Publications/Overseeing-Intelligence-Services-A-Toolkit

Parliamentary Oversight of Security and Intelligence Agencies in the European Union, Director General for Internal Policies, European Parliament, European Union (2011) available at:

http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf

The Intelligence and Security Committee, Dawson, J., Briefing Paper No. 02178, House of Commons Library (UK) (Feb. 2, 2016) available at http://researchbriefings.files.parliament.uk/documents/SN02178/SN02178.pdf

Office of the Inspector-General of Intelligence and Security Annual Report 2015 (NZ) (Oct 21, 2015) available at http://www.igis.govt.nz/assets/IGIS-Annual-Report-2015.pdf

External oversight of intelligence agencies: a comparison, Parliamentary Library of New Zealand (May 13, 2013) available at http://www.parliament.nz/en-nz/parl-support/research-papers/00PLLawRP13051/external-oversight-of-intelligence-agencies-a-comparison

SIPRI Yearbook 2007: Armaments, Disarmament and International Security (Oxford University Press: Oxford, 2007) (see Chapter 5: Democratic accountability of intelligence services) available at http://www.sipri.org/yearbook/2007/files/SIPRIYB0705.pdf

Legislation

Australian Security Intelligence Organisation Act (1979) available at https://www.legislation.gov.au/Details/C2016C00314

Intelligence Services Act (AU) (2001) available at https://www.legislation.gov.au/Details/C2008C00204

Canadian Security Intelligence Service Act (1985) available at http://lois-laws.justice.gc.ca/eng/acts/C-23/

Security Service Act (UK) (1989) available at http://www.legislation.gov.uk/ukpga/1989/5/contents

Intelligence Services Act (UK) (1994) available at http://www.legislation.gov.uk/ukpga/1994/13/contents

Justice and Security Act (UK) (2013) available at http://www.legislation.gov.uk/ukpga/2013/18/contents/enacted/data.htm

Inspector-General of Intelligence and Security Act (NZ) (1996) available at http://www.legislation.govt.nz/act/public/1996/0047/latest/DLM392285.html

Intelligence and Security Committee Act, (NZ) (1996) available at http://www.legislation.govt.nz/act/public/1996/0046/latest/DLM392242.html

Security Intelligence Service Act (NZ) (1969) available at http://www.legislation.govt.nz/act/public/1969/0024/latest/DLM391606.html

Newspaper Articles

I asked CSIS for its file on me. Here's what I got, Canada Star.com (May 8, 2015) available at http://www.thestar.com/news/privacy-blog/2015/05/what-happens-when-you-request-your-csis-file.html

Q&A:NSA's Prism internet Surveillance Scheme, BBC (Jun. 25, 2013) available at http://www.bbc.com/news/technology-23027764

Edward Snowden: Leaks that Exposed US Spy Programme, BBC (Jan. 14, 2014) available at http://www.bbc.com/news/world-us-canada-23123964

UK Intelligence Forced to Reveal Secret Policy for Mass Surveillance of Residents' Facebook and Google Use, Privacy International (Jun. 16, 2014) available at https://www.privacyinternational.org/node/469

GCHQ-NSA Intelligence Sharing Unlawful, Says UK Surveillance Tribunal, Privacy International (Feb. 6, 2015) available at https://www.privacyinternational.org/node/482

Canada's Spy Agencies Broke Surveillance Laws, Watchdogs Reveal, The Globe and Mail (Jan. 28, 2016) available at http://www.theglobeandmail.com/news/politics/spy-watchdog-says-ottawa-not-properly-policing-insider-threats/article28428602/

Canada's Top Court Strikes Down Police Powers to Wiretap Without Warrants, Canada Star.com (Apr. 13, 2012) available at http://www.thestar.com/news/canada/2012/04/13/canadas_top_court_strikes_down_police_powers_to_wiretap_without_warrants.html

APPENDIX

The below the listing of good practices on legal and institutional frameworks for intelligence services and their oversight found in the UN Report. Please refer to the substantive sections in the UN Report for a discussion of the particular provisions enacted in many jurisdictions. Critical sections have been emphasized below.

Practice 1. Intelligence services play an important role in protecting national security and upholding the rule of law. Their main purpose is to collect, analyse and disseminate information that assists policymakers and other public entities in taking measures to protect national security. This includes the protection of the population and their human rights.

Practice 2. The mandates of intelligence services are narrowly and precisely defined in a publicly available law. Mandates are strictly limited to protecting legitimate national security interests as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address. If terrorism is included among these threats, it is defined in narrow and precise terms.

Practice 3. The powers and competences of intelligence services are clearly and exhaustively defined in national law. They are required to use these powers exclusively for the purposes for which they were given. In particular, any powers given to intelligence services for the purposes of counter-terrorism must be used exclusively for these purposes.

Practice 4. All intelligence services are constituted through, and operate under, publicly available laws that comply with the Constitution and international human rights law. Intelligence services can only undertake or be instructed to undertake activities that are prescribed by and in accordance with national law. The use of subsidiary regulations that are not publicly available is strictly limited, and such regulations are both authorized by and remain within the parameters of publicly available laws. Regulations that are not made public do not serve as the basis for any activities that restrict human rights.

Practice 5. Intelligence services are explicitly prohibited from undertaking any action that contravenes the Constitution or international human rights law. These prohibitions extend not only to the conduct of intelligence services on their national territory but also to their activities abroad.

Practice 6. Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialized oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution that is independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices.

Practice 7. Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence.

Practice 8. Oversight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties are provided for the breach of these requirements by members of oversight institutions.

Practice 9. Any individual who believes that her or his rights have been infringed by an intelligence service is able to bring a complaint to a court or oversight institution, such as an ombudsman, human rights commissioner or national human rights institution. Individuals affected by the illegal actions of an intelligence service have recourse to an institution that can provide an effective remedy, including full reparation for the harm suffered.

Practice 10. The institutions responsible for addressing complaints and claims for effective remedy arising from the activities of intelligence services are independent of the intelligence services and the political executive. Such institutions have full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders.

Practice 11. Intelligence services carry out their work in a manner that contributes to the promotion and protection of the human rights and fundamental freedoms of all individuals under the jurisdiction of the State. Intelligence services do not discriminate against individuals or groups on the grounds of their sex, race, colour, language, religion, political or other opinion, national or social origin, or other status.

Practice 12. National law prohibits intelligence services from engaging in any political activities or from acting to promote or protect the interests of any particular political, religious, linguistic, ethnic, social or economic group.

Practice 13. Intelligence services are prohibited from using their powers to target lawful political activity or other lawful manifestations of the rights to freedom of association, peaceful assembly and expression.

Practice 14. States are internationally responsible for the activities of their intelligence services and their agents, and any private contractors they engage, regardless of where these activities take place and who the victim of internationally wrongful conduct is. Therefore, the executive power takes measures to ensure and exercise overall control of and responsibility for their intelligence services.

Practice 15. Constitutional, statutory and international criminal law applies to members of intelligence services as much as it does to any other public official. Any exceptions allowing intelligence officials to take actions that would normally violate national law are strictly limited and clearly prescribed by law. These exceptions never allow the violation of peremptory norms of international law or of the human rights obligations of the State.

Practice 16. National laws provide for criminal, civil or other sanctions against any member, or individual acting on behalf of an intelligence service, who violates or orders an action that would violate national law or international human rights law. These laws also establish procedures to hold individuals to account for such violations.

Practice 17. Members of intelligence services are legally obliged to refuse superior orders that would violate national law or international human rights law. Appropriate protection is provided to members of intelligence services who refuse orders in such situations.

Practice 18. There are internal procedures in place for members of intelligence services to report wrongdoing. These are complemented by an independent body that has a mandate and access to the necessary information to fully investigate and take action to address wrongdoing when internal procedures have proved inadequate. Members of intelligence services who, acting in good faith, report wrongdoing are legally protected from any form of reprisal. These protections extend to disclosures made to the media or the public at large if they are made as a last resort and pertain to matters of significant public concern.

Practice 19. Intelligence services and their oversight institutions take steps to foster an institutional culture of professionalism based on respect for the rule of law and human rights. In particular, intelligence services are responsible for training their members on relevant provisions of national and international law, including international human rights law.

Practice 20: Any measures by intelligence services that restrict human rights and fundamental freedoms comply with the following criteria:

(a) They are prescribed by publicly available law that complies with international human rights standards;

(b) All such measures must be strictly necessary for an intelligence service to fulfil its legally prescribed mandate;

(c) Measures taken must be proportionate to the objective. This requires that intelligence services select the

measure that least restricts human rights, and take special care to minimize the adverse impact of any measures on the rights of individuals, including, in particular, persons who are not suspected of any wrongdoing;

(d) No measure taken by intelligence services may violate peremptory norms of international law or the essence of any human right;

(e) There is a clear and comprehensive system for the authorization, monitoring and oversight of the use of any measure that restricts human rights;

(f) Individuals whose rights may have been restricted by intelligence services are able to address complaints to an independent institution and seek an effective remedy**.**

Practice 21. National law outlines the types of collection measures available to intelligence services; the permissible objectives of intelligence collection; the categories of persons and activities which may be subject to intelligence collection; the threshold of suspicion required to justify the use of collection measures; the limitations on the duration for which collection measures may be used; and the procedures for authorizing, overseeing and reviewing the use of intelligence-collection measures.

Practice 22. Intelligence-collection measures that impose significant limitations on human rights are authorized and overseen by at least one institution that is external to and independent of the intelligence services. This institution has the power to order the revision, suspension or termination of such collection measures. Intelligence collection measures that impose significant limitations on human rights are subject to a multilevel process of authorization that includes approval within intelligence services, by the political executive and by an institution that is independent of the intelligence services and the executive.

Practice 23. Publicly available law outlines the types of personal data that intelligence services may hold, and which criteria apply to the use, retention, deletion and disclosure of these data. Intelligence services are permitted to retain personal data that are strictly necessary for the purposes of fulfilling their mandate.

Practice 24. Intelligence services conduct regular assessments of the relevance and accuracy of the personal data that they hold. They are legally required to delete or update any information that is assessed to be inaccurate or no longer relevant to their mandate, the work of oversight institutions or possible legal proceedings.

Practice 25. An independent institution exists to oversee the use of personal data by intelligence services. This institution has access to all files held by the intelligence services and has the power to order the disclosure of information to individuals concerned, as well as the destruction of files or personal information contained therein.

Practice 26. Individuals have the possibility to request access to their personal data held by intelligence services. Individuals may exercise this right by addressing a request to a relevant authority or through an independent data-protection or oversight institution. Individuals have the right to rectify inaccuracies in their personal data. Any exceptions to these general rules are prescribed by law and strictly limited, proportionate and necessary for the fulfilment of the mandate of the intelligence service. It is incumbent upon the intelligence service to justify, to an independent oversight institution, any decision not to release personal information.

Practice 27. Intelligence services are not permitted to use powers of arrest and detention if they do not have a mandate to perform law enforcement functions. They are not given powers of arrest and detention if this duplicates powers held by law enforcement agencies that are mandated to address the same activities.

Practices 28 – 30 apply to the use of detention and arrest powers which are not applicable to the SSA.

Practice 31. Intelligence-sharing between intelligence agencies of the same State or with the authorities of a foreign State is based on national law that outlines clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence.

Practice 32. National law outlines the process for authorizing both the agreements upon which intelligence-sharing is based and the ad hoc sharing of intelligence. Executive approval is needed for any intelligence-sharing agreements with foreign entities, as well as for the sharing of intelligence that may have significant implications for human rights.

Practice 33. Before entering into an intelligence-sharing agreement or sharing intelligence on an ad hoc basis, intelligence services undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart. Before handing over information, intelligence services make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and will not be used for purposes that violate human rights.

Practice 34. Independent oversight institutions are able to examine intelligence-sharing arrangements and any information sent by intelligence services to foreign entities.

Practice 35. Intelligence services are explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities. If States request foreign intelligence services to undertake activities on their behalf, they require these services to comply with the same legal standards that would apply if the activities were undertaken by their own intelligence services.