Annex 2

to the

MEMORANDUM OF UNDERSTANDING

Between

THE COMMUNICATIONS SECURITY ESTABLISHMENT (herein referred to as CSE)

And

THE CANADIAN SECURITY INTELLIGENCE SERVICE (herein referred to as CSIS)

Regarding threat reduction activities pursuant to s.12.1 of the *CSIS Act*

1. REFERENCES

1.1. The MOU between CSIS and CSE, dated December 14, 2011 sets out an arrangement under s.17 of the *CSIS Act* for ongoing cooperation on information and intelligence collection, information sharing and operational support. This annex establishes a working agreement pursuant to paragraph 3.4 of the MOU.

2. PURPOSE

2.1. The purpose of this agreement is to establish the circumstances and the process by which CSIS will:

a) notify CSE of its use of s.12.1 threat reduction measures within Canada that may have an impact on CSE's activities pursuant to its mandate under the *National Defence Act* (*NDA*);

b) consult with CSE on its use of s.12.1 threat reduction measures in the global information infrastructure (GII); and,

c) request assistance from CSE in exercising its authority pursuant to s.12.1 of the *CSIS Act*.

2.2. While the agreement serves to ensure a common understanding by both CSIS and CSE on the process for consultation and for requesting and executing assistance, additional requirements or caveats may be included in the formal request submitted.

3. DEFINITIONS

3.1. In this MOU, the terms listed below, in singular or plural form according to the context, are defined as follows:

CSIS Threat Reduction Activity (TRA), also referred to as **s.12.1 threat reduction measures,** refers to an operational measure undertaken by CSIS, or by CSE acting pursuant to its assistance mandate, where the principal purpose is to reduce a threat to the security of Canada, as defined in s.2 of the *CSIS Act*.

GII has the same meaning as defined in the *NDA* and includes electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, systems, or networks. Examples include, but are not limited to, the Internet,

Notification refers to the process by which CSIS may advise CSE of its intended use of s.12.1 threat reduction measures. No formal response from CSE is required.

Consultation refers to the process by which CSIS will confer with CSE on its use of s.12.1 threat reduction measures in the GII to minimize adverse impacts on CSE . A formal response from CSE is required.

Cyber Security Investigations refers to the investigations conducted by the CSIS into the threats, motives and identity of foreign state actors which pose a threat to the security of Canada through the GII.

4. AUTHORITIES

4.1. *CSIS*

In accordance with the *CSIS Act*, CSIS may take measures to reduce threats to the security of Canada, as defined in s.2 of the *CSIS Act*. Specifically, the *CSIS Act* stipulates that:

> 12.1 (1) If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat;
>
> (2) The measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat; and,
>
> (3) The Service shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* or will be contrary to other Canadian law, unless the Service is authorized to take them by a warrant issued under section 21.1.
>
> (4) For greater certainty, nothing in subsection (1) confers on the Service any law enforcement power.

Pursuant to s.21.1 of the *CSIS Act*, the Director of CSIS or a designated employee may, with the approval of the Minister of Public Safety and Emergency Preparedness, apply for and obtain warrants to enable CSIS to reduce a threat to the security of Canada.

Pursuant to subsection 17(1) of the *CSIS Act*, CSIS may, with the approval of the Minister of Public Safety and Emergency Preparedness, enter into an arrangement or otherwise cooperate with any department of the government of Canada.

Pursuant to subsection 19(2) of the *CSIS Act*, CSIS may disclose information obtained in the performance of its duties for the purpose of performing its duties and functions under the Act, including advising the Government of Canada.

4.2. *CSE*

The mandate of the Communications Security Establishment is defined under section 273.64(1) of the *NDA*, authorizing CSE:

> (a) to acquire and use information from the GII for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
>
> (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada;

(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

In accordance with Ministerial direction authorizing CSE:

- under the request for assistance program, to provide technical and operational assistance, including and information processing and protection;
- provide non-communications information from electronic intelligence, (ELINT); and
- provide intelligence through its signals intelligence program, in response to broad Government of Canada and agency-specific intelligence priorities.

Under Ministerial direction, CSE is required to protect signals intelligence (SIGINT) capabilities and the interests of Canada's cryptologic allies.

5. ENGAGEMENT WITH CSE

5.1. *Notification*

a) CSIS will notify CSE of its s.12.1 threat reduction measures undertaken within Canada which have the potential to directly or indirectly affect CSE's mandated activities Such notification will occur via CSIS Headquarters to CSE's SIGINT Policy and Review (SPR) group and both parties agree to document such discussions to respective files.

b) Where such notification is provided, CSIS will also advise CSE on circumstances when information relating to the s.12.1 threat reduction measure may be disclosed and/or should be disclosed by CSE along with any related caveats or handling instructions.

5.2. *Consultation*

a) CSIS will consult with CSE on s.12.1 threat reduction measures when any of the triggers for consultation are met (see Appendix 1).

b) As part of CSIS's planning process, CSIS shall, where possible, engage with relevant counterparts at CSE to discuss the nature of the threat-related activity and proposed s.12.1 threat reduction measure as well as the intended goal. Where both CSIS and CSE have strategic interests relating to the nature of the threat-related activity (e.g. cyber

security investigations), these discussions may also consider the strategic value of the proposed measure and whether alternatives may be more suitable. These discussions also provide an opportunity for CSE to provide a preliminary assessment on any foreseeable adverse impacts to CSE

c) Further to these discussions and in advance of CSIS seeking internal approval on the proposed measure, the will send a formal request for consultation to CSE's SPR, which will also contain any information sharing restrictions relevant to CSE's potential engagement of As CSE acts as the representative, in Canada, of

d) Where CSE identifies significant concerns related to a consultation trigger listed in Appendix 1, all relevant CSIS and CSE stakeholders, including CSIS and CSE SPR, will be engaged to discuss the concerns and to accommodate the issues if possible. Where there is disagreement that remains unresolved, the matter will be referred for a more senior level discussion.

e) In a timely manner, SPR will either advise CSIS of any issues that could compromise equities and provide suggestions for alternative ways forward (as applicable) or indicate that there are no objections associated with the proposed measure.

5.3. *Requests for Assistance: CSE-enabled TRA*

a) CSIS may request CSE's assistance to reduce a threat to the security of Canada. Where possible, CSIS will engage CSE prior to submitting a request for assistance in order to facilitate the development of the request and related operational planning.

b) Specifically, both CSIS and CSE will engage in discussions, either secretarially or in person, to identify possible measure(s) for use against particular threat activities and to discuss related technical capabilities, requirements and any other relevant considerations.

c) If CSIS anticipates that the execution of the measure will require a warrant, these discussions will also serve as an opportunity to identify what authorities may be required. To support the preparation of CSIS's affidavit, CSE must also provide CSIS with relevant technical details relating to how the measure will be executed and whether the is anticipated.

d) The aforementioned discussions will serve to inform the development of a request for assistance, which the will forward to CSE in accordance with the process established by CSIS and CSE.

e) In order to consider providing assistance to CSIS, CSE is required to meet its obligations as outlined in Ministerial direction and/or CSE policy, including that CSE:

- receive a request in writing;
- be satisfied that CSIS has the lawful authority to conduct the activity requested; and,
- be assured that any information provided for the purpose of said assistance has been lawfully obtained by CSIS.

f) Where CSIS requires CSE's assistance to execute a s.12.1 threat reduction measure, CSIS will submit a formal request for assistance in writing to CSE. The request for assistance will provide sufficient information to enable CSE to verify that the lawful authority exists (including the warrant if applicable), and will also note any restrictions that CSE must conform to in providing the operational or technical assistance requested.

g) While respecting the obligations of CSE's Ministerial direction that cryptologic capabilities and the interests of Canada's cryptologic allies are protected, CSE will provide the Service as much information as possible regarding the means by which CSE will undertake the technical or operational assistance to enable CSIS to verify that CSE activities conform to its legal and administrative requirements.

h) As part of the request for assistance, CSIS will include:

- a statement of the applicable legislative authority, including relevant information from a warrant obtained pursuant to s.21.1 of the *CSIS Act*;
- any caveats or handling instructions relevant to the execution of the s.12.1 threat reduction measure;
- the period of time in which the measure must be executed (i.e. validity period of the approval);
- reporting requirements (e.g. confirmation the measure was undertaken, indication as to whether the immediate outcome was achieved); and,
- any other requirements, as applicable.

i) Upon receipt of the request for assistance, CSE will review and process the request and will provide a response to CSIS in a timely manner. Where CSE agrees to provide assistance, CSE agrees to abide by the requirements outlined in the request for assistance. In instances where CSE determines that it is unable to provide assistance, CSE agrees to provide CSIS a written response outlining the rationale for its decision.

j) Both parties agree to notify the other of any changes in the circumstances relating to the execution of the s.12.1 threat reduction measure (e.g. operational feasibility or technical landscape) as soon as possible. This will allow an assessment of any implications, including whether CSIS needs to seek additional authorization, either internally or from the Federal Court.

k) Where the nature of the change would require CSE to undertake activities that fall outside the scope of the original request for assistance, CSE will cease all assistance activities until such time as a new request for assistance is submitted by CSIS.

6. EFFECT, AMENDMENT, RENEWAL AND TERMINATION

6.1. This agreement:

- will enter into force once both parties have signed;
- may be amended at any time upon mutual consent of the parties, effected by an exchange of letters;
- may be terminated at any time by either of the parties, effective upon receipt of written notification; and
- will be reviewed and renewed on every two years from the date of signature.

The Terms of this Annex have been agreed upon by both parties.

Deputy Director Operations
Canadian Security Intelligence Service

June 13, 2016
Date

Shelly Bruce
Deputy Chief SIGINT
Communications Security Establishment

2016.6.13
Date

Appendix 1

Triggers requiring CSIS to consult with CSE on TRA

CSIS will consult with CSE prior to undertaking s.12.1 threat reduction measures under the following conditions:

1. When the proposed s.12.1 threat reduction measure uses or relies on SIGINT - derived information;

2. When the proposed activities targeted by the s.12.1 threat reduction measure are a threat to the GII;

3. When the proposed s.12.1 threat reduction measure seeks to

4. When the proposed s.12.1 threat reduction measure involves any Government of Canada systems or networks, or those of importance to the Government of Canada.

In certain circumstances where
CSIS and CSE have pre-existing agreements and mechanisms to consult with each other in real time. In these circumstances, the implicated operational areas will not be required to submit formal consultation notices in writing via DDO Sec and SPR *prior* to undertaking a s.12.1 threat reduction measure; however the operational areas will be required to track these consultations for review purposes.

Please note, at any time CSIS may engage with CSE to discuss possible s.12.1 threat reduction measures whether they be measures against Canadians or non-Canadians, in Canada or abroad. In the case where consultation is required or a request for assistance will be made, engagement of CSE at the earliest opportunity is appropriate.

The triggers for consultation in the Annex may be updated or edited at any time, provided both parties agree to the changes.