DIRECTIVE

FROM THE CHIEF OF THE COMMUNICATIONS SECURITY ESTABLISHMENT

THREATS TO DEMOCRACY

This Directive is issued by me, as the Chief of the Communications Security Establishment (CSE), to the Deputy Chief, Signal Intelligence (SIGINT), and the Head, Canadian Centre for Cyber Security (CCCS). Protecting Canada's democracy is one of the core responsibilities of the Government of Canada, and CSE plays an instrumental role in helping to fulfill that responsibility. As such, in this Directive, I have outlined my expectations on how CSE will contribute to broader Government of Canada efforts.

CSE will make vital contributions by continuing to exercise all aspects of its mandate to:

- **Detect** threats to Canada's democracy through foreign intelligence collection;
- **Defend** against threats to Canada's democracy through cybersecurity measures;
- **Disrupt** foreign threats to Canada's democracy by conducting foreign cyber operations; and,
- **Assist** other government departments in the lawful exercise of their mandates.

Ensuring foreign intelligence on threats to Parliament, Parliamentarians, their families and staff and cyber security threats linked to specific Parliamentarians gets into the right hands at the right time to inform decision making is a critical part of the work CSE does. Specifically, CSE will continue to:

- Ensure the timely dissemination of its products to the appropriate consumers of such intelligence, such as Security and Intelligence Threats to Elections Task Force (SITE), the House of Commons[1], relevant Deputy Minister-level committees, (and subordinate Assistant Deputy Minister fora,) as well as any other current or future fora seized with this issue as appropriate.

- Leverage existing dissemination mechanisms and support any future mechanisms established. In addition, CSE will be particularly mindful of supporting the Canadian Security Intelligence Service, as appropriate under the CSE Act, in carrying out their lawful duties pursuant to the Minister of Public Safety's Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians.

- Track and centrally record readership of CSE products.

[1] Engagement with House of Commons will be conducted in a manner which fully respects the independence of the legislative branch of government.

All CSE activities will be conducted in accordance with the *Communications Security Establishment Act* and in a manner consistent with the following principles:

- **Lawfulness** – CSE will apply the principles and requirements of the Canadian laws, legislation, and policies that drive us, including respecting and protecting the privacy of Canadians.
- **Transparency** – CSE will recognize that it is essential to democracy that Canadians understand what the Government does to protect national security, how the Government does it, and why such work is important.
- **Accountability** – CSE will support accountability measures, which are fundamental to Canada's system of government and maintaining the confidence of Canadians. CSE's accountability extends to the Minister of National Defence and to Cabinet, Parliament, and Canadians.

EFFECTIVE DATE: The Directive will take effect on the date of the signature.

Issued at OTTAWA this 8 day of September 2023.

Caroline Xavier
Chief

DIRECTIVE DE LA CHEF DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

MENACES CONTRE LA DÉMOCRATIE

En tant que chef du Centre de la sécurité des télécommunications (CST), je suis l'auteure de la présente directive, à l'intention de la chef adjointe, Renseignement électromagnétique (SIGINT) et du dirigeant principal du Centre canadien pour la cybersécurité (CCC). Protéger la démocratie du Canada est l'une des principales responsabilités du gouvernement du Canada et le CST joue un rôle clé pour aider à assumer cette responsabilité. Par conséquent, dans cette directive, je présente mes attentes sur la façon dont le CST contribuera aux efforts du gouvernement du Canada.

Le CST apportera une contribution essentielle en continuant d'exercer tous les volets de son mandat visant à :

- **Détecter** les menaces contre la démocratie du Canada en recueillant du renseignement étranger;
- **Défendre** la démocratie du Canada contre les cybermenaces grâce à des mesures de cybersécurité;
- **Contrer** les menaces étrangères contre la démocratie du Canada en menant des cyberopérations étrangères; et
- **Assister** les autres ministères dans l'exercice des mandats que la loi leur confère.

S'assurer que le renseignement étranger sur les menaces contre le Parlement, les députés, leurs familles, leur personnel, et les cybermenaces contre des députés en particulier, soit transmis aux bonnes personnes, en temps opportun, pour éclairer la prise de décisions est un élément essentiel du travail effectué par le CST. Plus précisément, le CST continuera de faire ce qui suit :

- Assurer la diffusion en temps opportun de ses produits aux clients qui ont besoin du renseignement, comme le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (GT MSRE), la Chambre des communes[1], les comités pertinents au niveau des sous-ministres (et les forums des sous-ministres adjoints subordonnés) ainsi que tout autre forum actuel ou futur saisi de cette question, le cas échéant.

- Tirer parti des mécanismes de diffusion et soutenir les mécanismes qui seront mis en place à l'avenir. De plus, le CST soutiendra particulièrement le Service canadien du renseignement de sécurité, conformément à la *Loi sur le CST*, dans l'exercice de ses fonctions conférées par la loi, à l'appui des Directives ministérielles sur les menaces à la sécurité du Canada dirigées contre le Parlement et les parlementaires du ministre de la Sécurité publique.

[1] La collaboration avec la Chambre des communes se fera d'une manière qui respecte pleinement l'indépendance du pouvoir législatif du gouvernement.

- Faire le suivi et consigner de manière centralisée le lectorat des produits du CST.

Toutes les activités du CST seront menées conformément à la *Loi sur le Centre de la sécurité des télécommunications* et de manière à respecter les principes suivants :

- **Respect de la loi** – Le CST applique les principes et les exigences qui découlent des lois canadiennes, du cadre législatif et des politiques régissant nos activités, y compris le respect et la protection de la vie privée des Canadiennes et Canadiens.
- **Transparence** – Le CST reconnaît qu'il est essentiel à la démocratie que les Canadiennes et Canadiens comprennent ce que le gouvernement fait pour protéger la sécurité nationale, comment il le fait et pourquoi un tel travail est important.
- **Reddition de comptes** – Le CST appuie les mesures de reddition de comptes qui sont essentielles au système de gouvernement du Canada et au maintien de la confiance des Canadiennes et Canadiens. Le CST rendra des comptes au ministre de la Défense nationale, au Cabinet, au Parlement et aux Canadiennes et Canadiens.

DATE D'ENTRÉE EN VIGUEUR : La présente directive entrera en vigueur à la date de la signature.

Publié à Ottawa, en ce 8 Septembre 2023.

Caroline Xavier
Chef