Public Inquiry Into Foreign Interference
in Federal Electoral Processes and
Democratic Institutions

Enquête publique sur l'ingérence étrangère
dans les processus électoraux et les
institutions démocratiques fédéraux

Interview Summary: Senate Administration (David Vatcher, Julie Lacroix and Shaila Anwar)

Three representatives from the Administration of the Senate of Canada (the "**Senate**"), David Vatcher, Director of Information Services, Julie Lacroix; Director of Corporate Security; and Shaila Anwar, Clerk of the Senate and Clerk of the Parliaments, were interviewed by Commission Counsel on 12 September 2024. Lawyers from the Office of the Law Clerk and Parliamentary Counsel of the Senate was present.

Notes to Readers:

- Commission Counsel have provided explanatory notes in square brackets to assist the reader.

1. Background

1.1 Shaila Anwar, Clerk of the Senate and Clerk of the Parliaments

[1] Ms. Anwar has been Clerk of the Senate and Clerk of the Parliaments since May 6, 2024. She joined the Senate in February 2007 as a procedural clerk.

1.2 Julie Lacroix, Director, Corporate Security Directorate ("CSD")

[2] Ms. Lacroix is the Senate's Director of Corporate Security. CSD is part of the Legislative Services division of the Senate Administration. She joined the Senate in 2015 as a senior advisor for Real Property and Security. Ms. Lacroix has a staff of 43 people, all with Top Secret security clearance.

1.3 David Vatcher, Director, Information Services Directorate ("ISD")

[3] Mr. Vatcher has been the Senate's Director of Information Services since 2018. The ISD forms part of the Corporate Sector of the Senate Administration. Serving both senators and senate employees, Mr. Vatcher is responsible for IT management and information management. Before joining the ISD, he was with Loto Québec for 23 years and worked

briefly for Fisheries and Oceans Canada. He has a staff of 52 people, all of whom have Secret security clearance.

2. Structure of the Senate Administration

2.1 Organization

[4] The Clerk of the Senate and the Clerk of the Parliaments lead the Senate administration. The Senate Administration has three sectors:

a. Legislative Services led and overseen by the Deputy Clerk;

b. the Legal Sector, led and overseen by the Law Clerk and Parliamentary Counsel; and

c. the Corporate Sector, led and overseen by the Chief of Corporate Services who is also the Clerk of the Standing Committee on Internal Economy, Budgets and Administration.

[5] The Legislative Services sector is composed of six directorates: the CSD led by Ms. Lacroix; the Office of the Usher of the Black Rod; the Chamber Operations and Procedure Office; the Committees Directorate, the Communications, Broadcasting and Publications Directorate and the International and Interparliamentary Affairs Directorate. The Usher of the Black Rod is responsible for security inside the Senate chamber when the Senate is in session.

[6] The Corporate Sector has three directorates: the Finance and Procurement Directorate, Property and Services, and Information Services, headed by Mr. Vatcher.

2.2 Standing Committee on Internal Economy, Budgets and Administration (CIBA)

[7] Under Rule 12-7(1) of the *Rules of the Senate* and S. 19.3 of *the Parliament of Canada Act*, CIBA considers, on its own initiative, all financial and administrative matters concerning the Senate's internal management. The committee is also authorized to act on all financial, and administrative matters concerning the internal administration of the

Senate, and to advise and rule on the use of Senate resources, subject to the Senate Administrative Rules.

[8] CIBA is chaired by Senator Lucie Moncion. CIBA has 15 senators from recognized parliamentary groups and recognized parties in the and two *ex officio* members: the Government Leader in the Senate or their representative; and the Opposition Leader in the Senate or their representative. Members of CIBA are put forward through a report proposed to the Senate by the Selection Committee. When the Senate adopts this report, senators are formally appointed to the CIBA, which then elects a president. [1] CIBA's composition approximately reflects the groups and parties in the Senate, which is reflected in the report by naming senators based on their affiliation to a recognized group or entity. Currently, the Independent Senators Group has four members on CIBA, the Conservative Party of Canada has three members, while the Canadian Senators Group and Progressive Senate Group each have two members.

2.3 Corporate Security Directorate

[9] CSD ensures the security of the Senate by organizing, directing and managing administrative and technical security programs of the Senate. The CSD also acts as the main strategic advisor to the President of the Senate, the senators and the Clerk of the Senate for all matters of institutional security as well as plans and measures relating to physical security. The CSD is responsible for all aspects of security except for physical security operations.[2] Everything else is under Ms. Lacroix's remit, which includes accreditation, parking, fire prevention, building access, administrative investigations, risk management, business continuity, event management (security), residence security, security for senators travelling abroad and within Canada, technical equipment operations (e.g. cameras) and security project management.

[1] *Senate Administrative Rules / Règlement administratif du Sénat*
[2] Parliamentary Protective Service is responsible for physical security.

[10] The Director of CSD interacts with the Usher of the Black Rod on security et decorum matters within the Senate chamber when the Senate is in session.

[11] CSD also works with the Sergeant-at-Arms of the House of Commons with respect to anything involving the use of Parliament Hill.

[12] The CSD collaborates closely with the Sergeant-at-Arms of the House of Commons and the Director of the Parliamentary Protective Services.

[13] CSD has security training for senators and to employees. Before senators and employees travel, it also gives them specific training related to their travel plans and meets with senators on their return. CSIS and Public Safety Canada provide information to CSD for its training.

2.4 Information Security Directorate

[14] ISD is responsible for Senate IT equipment such as computers, telephones, servers and switches, for all senators and Senate employees, as well as ensuring that all of the Senate's equipment is secure.

[15] ISD gives training, which includes simulation exercises, to senators and employees. Within the first two weeks of starting employment, all employees must have this training. Mr. Vatcher meets one on one with senators to explain security risks.

[16] ISD also provides phishing detection services, among other IT services.

3. CSD and ISD engagement with foreign interference

3.1 Generally

[17] CSD has a few units that may engage on foreign interference issues.

[18] The accreditation unit is responsible for ensuring senators and staff are accredited and are not security risks.

[19] There is a Technical Countermeasures unit that provide sweeping services.

[20] CSD provides senators with non-classified briefings and material about foreign interference, such as the document prepared by CSIS entitled "Far From Home" gives

them advice about foreign interference risks when they travel. CSD also provides briefings to Senate groups and caucus meetings.

[21] ISD also has guidelines for senators when they travel and asks senators to contact ISD before they travel. ISD then performs a risk assessment based on where senators are travelling to and who they are meeting with.

[22] CSD shares open-source information daily with, and receives information from, House of Commons, the RCMP, CSIS, local police and Global Affairs Canada.

[23] ISD has a team who deal with cybersecurity and information technology (IT) security. IT-related foreign interference issues are brought to this team. Any security or cybersecurity incident can have an element of foreign interference.

[24] ISD also deals with "Distributed Denial-of-Service" (DDoS) attacks.[3] Given their temporary nature, these attacks did not stop senators from doing their work. The overall budget of the ISD includes funds to mitigate a variety of risks and to implement threat-minimizing measures. DDoS attacks do not result in attackers gaining access to Senate information because its internal network is strongly protected. ISD knows that last year's DDoS attacks were conducted by Russian sympathizers based on technical information and reporting on social networks. When DDoS attacks occur, ISD does not usually need to contact security and intelligence partners because it has the capabilities to handle them on its own.

[25] Mr. Vatcher explained that perpetrators of cyberattacks can be grouped in 4 categories, from those with the least resources to the most resources at their disposal: opportunists, activists, criminals and state actors. The biggest threats are those with significant funding and time to invest in attacks, which results in more sophisticated attacks.

DDoS attacks does not impede the institution's ability to carry out its work.

[3] This occurs when a cyber attacker floods a server with Internet traffic to prevent users from accessing connected online services and sites. "Zombie" machines, i.e., poorly protected machines, receive a command to make requests to websites. These sites then receive a high level of traffic and cannot handle the requests. The result is the site is overwhelmed and users cannot access the site.

3.2 APT 31 incident

[26] ISD was informed in January 2021 about a "spear phishing" activity targeting parliamentary accounts, including Senate accounts, later attributed to an organization known as "APT 31."

[27] During the initial attack in January 2021, ISD was informed that suspicious emails were being sent to senators. It was unusual for an external partner to warn ISD about a cyberattack; ISD is normally capable of predicting and preventing cyberattacks using its own resources. However, some of these emails did make it through the Senate's firewalls and landed in some senators' inboxes. The senators' offices were immediately contacted to ensure any emails received were destroyed. ISD also did a search of the Senate email database to ensure emails were deleted. The attack failed because most emails were caught by the firewalls, and no one opened the emails that did make it through; attackers did not gain access to any information from the Senate's servers.

[28] At that time, ISD was only aware that malware was sent in an email. It did not know whether the attack was conducted by APT 31 acting on behalf of the People's Republic of China (PRC).

[29] ISD learned in June 2024 from the House of Commons IT security team that the attack was conducted by APT 31. In any event, knowing the source of the attack earlier would not have changed ISD's prompt response.

[30] The Canadian Centre for Cyber Security did not provide any information to the Senate Administration in 2024 on who may have been behind the attacks, despite public statements to the contrary by other organizations in 2024.

3.3 New Procedures in Response to Foreign Interference

[31] CSD has revised its security accreditation policy. It now requires certified-criminal record checks using digital fingerprints in 2023. Previously, it did name-based criminal record checks. Security interviews and resolution of doubt interviews are as necessary.

[32] ISD does not have any new procedures specific to foreign interference.

4. Senate Relationship with the House of Commons

[33] The Senate and the House of Commons share a computer network, and there is an agreement delimiting each chamber's responsibilities.

5. Senate Relationship with the Government of Canada

5.1 CSD relationships with government organizations

[34] CSD works with law enforcement and intelligence agencies as part of its regular operations, both proactively and in response to specific incidents, some of which can involve foreign interference issues.

[35] CSD and security and intelligence agencies exchange information about possible threats to the Senate. An example of an incident-based interaction could be in an accreditation case, where CSD discusses or exchanges information with its security and intelligence partners if adverse information is discovered during the accreditation process.

[36] CSD also has regular briefing sessions with CSIS and other security and intelligence partners. CSD engages frequently with CSIS. CSD has a strong collaborative relationship with CSIS on many issues, not just foreign interference. CSD and CSIS usually meet at least once every quarter and sometimes more frequently, depending on what is happening in the world or with respect to either organization. The quarterly meetings with CSIS may sometimes include the RCMP, depending on what is being discussed.

[37] Sometimes CSD meets with multiple agencies and attends forums with all partners. INTERSECT is a monthly meeting CSD attends with a variety of partners.

[38] Foreign interference is now a more frequent topic of discussion between CSD and its security and intelligence partners.

[39] CSD's open-source data collection unit collaborates with various partners, including the RCMP, local police and Global Affairs Canada.

[40] CSD collaborates with CSE, the House of Commons, ISD and the RCMP on cyber threats.

5.2 ISD relationships with government organizations

[41] ISD tries to be as proactive as possible in preventing cyberattacks, and to that end, has implemented several best practices recommended by the Canadian Centre for Cyber Security.

[42] Government entities sometimes contact ISD to say there is a risk about a country or group that could impact the Senate. ISD has regular conversations with security and intelligence partners but fewer in-person meetings than CSD has with security and intelligence partners. ISD communicates with security and intelligence partners more frequently over telephone or email. Partners inform ISD about security or cybersecurity incidents.

[43] ISD is satisfied with the information it gets from its security and intelligence partners. ISD's relationships with its partners are very positive and there is good collaboration.

[44] ISD's practices ensure risks are addressed very quickly to avoid incidents becoming more serious, but Mr. Vatcher noted that part of ISD's work will always be reactive. That is the nature of the industry and issues therein, not because there is a lack of information.

5.3 Arrangements with government organizations

[45] The Senate and the House of Commons have a memorandum of understanding (MOU) with the RCMP and Public Safety Canada with respect to the Parliamentary Protective Service.

6. Access to Classified Information

6.1 Receiving classified information

[46] CSD sometimes receives classified information. It has received classified information from the Government of Canada about foreign interference.

[47] ISD does not usually receive classified information. If it does, distribution is limited on a need-to-know basis. ISD has not received any classified information about foreign interference.

6.2 Handling classified information

[48] The Senate has physical infrastructure to process and engage with classified information.

[49] Senate networks allow users to access the Internet so there is no Top Secret information stored on them.

7. Security and Employees

7.1 All employees

[50] All employees of the ISD, contractors and students go through an accreditation process and need, at a minimum, a Secret level security clearance by CSIS.

[51] All CSD employees, contractors and students go through an accreditation process and need, at a minimum, a Top Secret security clearance by CSIS.

[52] Site access for employees, contractors and students is very similar to an Enhanced Reliability security clearance but also includes a loyalty to Canada component.

7.2 Senatorial staff

[53] Senators have a budget and are responsible for hiring their staff, who become Senate employees. Staff working in the office of a senator work under the direction of their senator, who acts as their manager. Staff are subject to Senate policies and receive Senate equipment.

[54] Staff must be accredited by CSD, who works together with CSIS to evaluate candidates' security profiles. CSD can refuse accreditation, including due to foreign interference concerns.

8. Information Technology Services for Senators

8.1 Equipment

[55] Each senator's office is entitled to four laptops. If a senator wants to buy an additional computer for Senate business, they must get authorization to connect it to the Senate network.

[56] There are also limits on printers and mobile phones. For the latter, each employee can only have one. Each senator's office can have up to 10 components of a plan (e.g., data, voice calling, etc.) Senators can choose not to have a mobile phone. ISD installs device managers on every phone so they can be managed remotely.

[57] The Senate Administration is not responsible for personal phones or plans or digital accounts (e.g. Gmail, Facebook). However, if there is a cyberattack involving a senator or employee, even if this attack falls outside of Senate jurisdiction, ISD will still do what it can to minimize the impact on a best-efforts basis, including leveraging institutional relationships with social media platforms.

8.2 Cyber attacks

[58] There are cyberattacks on the Senate every day – spam, malware, ransomware, etc. Cyberattacks continue to grow significantly, both in number and in sophistication.

[59] ISD continuously checks Senate vulnerability to cyberattacks and intervenes if it finds a problem. Rarely do any cyberattacks succeed. This is mostly because the Senate is aware of the threats they face and these attacks are foreseeable; in other words, the Senate knows how it is often targeted. Accordingly, it has the tools and processes to contain attacks before they develop into larger incidents. An example of a growing vulnerability is "secondary" attacks, which are cyberattacks on a trusted institution or person.

[60] With many people working remotely, the challenge for IT security has evolved from a closed centralized network to a network with multiple remote access. This evolution of the security challenge has necessitated new protection tools, as well as new habits.

[61] ISD has plans to add to its cyber security based on the need of senators. Senators have identified cyber security as one of the Senate's most important risks.

8.3 Misinformation

[62] ISD makes best efforts to respond to any attempt to impersonate a senator (social media, personal email addresses), even if it is not within ISD's areas of responsibility.

9. Physical Security for Senators

[63] The Parliamentary Protective Service oversees physical security operations on Parliament Hill for all parliamentarians. This includes securing the perimeter of the parliamentary precinct. Senators can readily reach security officials if their physical safety is under threat.

[64] CSD detects threats to senators through various means. In some instances, threats are directly received by senators. In other instances, threats are detected through OSINT collection, intelligence received from partner agencies and information from law enforcement agencies.

10. Regional offices

[65] Senators can establish a regional office in their home province within the budgets prescribed in the Policy on Management of Senators' Offices. Only four senators out of 100 have regional offices currently. All arrangements are made by the senators and are not the responsibility of the Senate. The Senate's involvement is limited to advice.

11. Senate Motion About Sponsored Travel

[66] Senator Raymonde Saint-Germain put forward a notice of motion proposing that the Senate Sanding Committee on Ethics and Conflicts of Interest be authorized to study changes to regulations around sponsored travel.[4] This motion is currently undergoing the adoption process in the Senate.

[67] The notice of motion was introduced last spring following stories about foreign interference in the news that followed the 2024 classified report on foreign interference by the National Security and Intelligence Committee of Parliamentarians.

[4] Senate of Canada Institutional Report, SEN0000001.EN at p. 16 [the French institutional report can be found at SEN0000001.FR].

12. Recommendations

[68] Witnesses had no recommendations to propose to the Commission at this time. Witnesses stated that their roles are to fulfil their duties to the best of their ability, according to directions provided and decisions made by senators, and within the budget that they have.