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: House of Commons Administration (Patrick McDonell and Benoît Dicaire)

Patrick McDonell, Sergeant-at-Arms, and Benoît Dicaire, Chief Information Officer for the House of Commons were interviewed by Commission Counsel on September 3, 2024.

Notes to Readers:

- Commission Counsel have provided explanatory notes in square brackets to assist the reader.
- This interview was conducted bilingually. The language used in the summary reflects the language in which answers were given.
- Cette entrevue a été menée de manière bilingue. La langue employée dans le résumé correspond à la langue dans laquelle les réponses ont été données.

1. Introduction

[1] Patrick McDonell is the current Sergeant-at-Arms and Corporate Security Officer of the House of Commons (the "**House**" or "**HOC**"). On top of performing many ceremonial duties, he is responsible for the security of the House and its members in the Chamber and when they are off of the Parliamentary precinct. This includes the constituency offices and private residences of members of Parliament ("**MPs**"). He oversees a team of about 114 employees.

[2] He was formally appointed to his position in July 2019, previously serving as acting Sergeant-at-Arms, following the appointment of Kevin Vickers as ambassador to Ireland in 2015. He joined the RCMP in 1980, serving in various capacities, before moving to the Senate of Canada, where he was Director of the Senate Protective Service.

[3] Benoît Dicaire is the current Chief Information Officer ("**CIO**"), Digital Services and Real Property ("**DSRP**"), of the House. He heads a team of 760 employees that oversees and provides IT security infrastructure, applications and support to the House, its members

and employees, and is responsible for IT security policy and cybersecurity. He is also responsible for technology integration in the facilities of the HOC as well as broadcasting and webcasting when HOC is in session. Part of the CIO'S mandate is to protect parliamentary information.

[4] Mr. Dicaire has been with HOC for 24 years and was appointed to his current position in 2024. He holds a Bachelor of Commerce from the University of Ottawa.

2. Structure of the House of Commons Administration

[5] The Board of Internal Economy ("**BOIE**") is the entity responsible for all financial and administrative matters for the HOC, its premises, services and employees, and MPs. It is created by the *Parliament of Canada Act*. The BOIE is chaired by the Speaker of House, who is selected by all MPs. Membership in BOIE is divided equally between government and opposition MPs. The number of members changes depending on the number of recognized parties in the House. Currently, there are four recognized parties. The official opposition gets two members, and each other opposition party gets one member each. The governing party thus has four members.

[6] The BOIE makes by-laws pertaining to the management of HOC resources by MPs. The BOIE enforces its own by-laws but the House Administration plays an active role in their implementation. For example, the finance department processes expense claims from all members. The department must determine whether the expense being claimed relates to parliamentary business, which can sometimes be challenging. HOC administration processes over 100,000 claims per year.

[7] There are no units within either the offices of the Sergeant-at-Arms or the Chief Information Officer that deal specifically with foreign interference, but it is relevant to the work of some units, such as the Risk Management & Investigations unit.

[8] The Open-Source Monitoring Program also falls under the responsibility of the Sergeant-at-Arms. This includes a team of analysts who monitors open-source intelligence ("**OSINT**") for threats and harassment towards MPs. If they come across conduct that could be criminal, they communicate with either the RCMP or relevant

police of jurisdiction. There is standard collaboration between the Sergeant-at-Arms' team and HOC IT services.

[9] The Office of the Sergeant-at-Arms has an investigative unit, composed mostly of former police officers, that investigates cases of threats and harassment of MPs. Another team within the Office conducts counter technical investigations, including monitoring signals and sweeping for bugs [covert monitoring devices].

[10] The Parliamentary Protective Service ("**PPS**") is a separate entity from the HOC administration and falls under the responsibility of both the Speakers of the HOC and the Senate. The Director of the Service is a member of the RCMP. It has a specific mandate for institutions of Parliament, not just the House. It is responsible for the physical security of MPs while on the Parliamentary Precinct.

3. IT Security Measures and Policies

[11] From a technological point of view, Mr. Dicaire explained that there are various rules that govern what MPs have and what they can do on their HOC electronic devices. There is a BOIE Acceptable Use Policy from 2014 that dictates acceptable and unacceptable behaviour and an IT security policy from 2016. There is also an Information Management Policy that was recently updated in 2024, that currently applies to HOC staff, but not MPs, as it has yet to be endorsed by BOIE.

[12] The IT security program is based on both proactive and reactive measures, which involves both incident monitoring and reporting from various sources, including complaints. It adopts a multilayered approach based on industry standards and best practices intended to reduce risk at every level and to ensure MPs can conduct their business efficiently whether in caucus, at their constituency office or in the chamber. There are controls in place at the device and user level, as well as perimeter controls.

[13] Mr. Dicaire explained that from an IT perspective, the House has its own infrastructure and manages its own networks. Perimeter controls ensure the infrastructure itself is protected at the perimeter, including at points of contact with the internet as well as

Government of Canada networks. The HOC network is designed so that it complies with international standards.

[14] Members of Parliament have a duty to report to the House Administration when they travel internationally with a HOC electronic device, regardless of the purpose of the trip. All HOC devices are tracked, and DSRP can tell when a device is outside the country. If an MP is not carrying a HOC device abroad, there is no duty to advise House administration. Reports are generated every morning to see where various MPs around the world are when travelling with a HOC device.

[15] Various measures can be taken when an MP travels abroad with a HOC device without informing House Administration. This could involve contacting the non-compliant MP to remind them of the issue, and/or escalate the matter to the relevant party whip. DSRP has the capability to interrupt access to the device, especially where the MP is visiting a country of concern to Canada. The CIO has the obligation and the discretion to interrupt access if he believes there is a particular risk.

3.1 HOC electronic devices provided to MPs and cybersecurity

[16] M. Dicaire a expliqué que les députés se font remettre trois ordinateurs pour les bureaux sur la Colline parlementaire. Pour les bureaux de comté, ils peuvent avoir jusqu'à 10 appareils électroniques fournis par la Chambre des communes (la « **Chambre** » ou « **CC** »). Les députés ne peuvent pas utiliser des appareils non-autorisés par l'administration de la Chambre. Des dispositions sont prévues pour certains appareils personnels (e.g. les Macbook). Ils peuvent se brancher sur un réseau « invité », qui est également sécurisé. En ce qui concerne les appareils portables, il peut y en avoir un par employé.

[17] Lorsque les députés voyagent à l'étranger, ils bénéficient du programme « ParlVoyage ». Ce programme prévoit une évaluation du risque effectuée en fonction de la destination du voyageur et des personnes qui l'accompagnent. Suivant cette évaluation, le droit de voyager avec les appareils électroniques parlementaires est soit accordé ou, s'il existe un risque à la sécurité, l'appareil est restreint avec une différente

configuration de sécurité. L'expérience utilisateur demeure néanmoins similaire et le député conserve l'accès à ses courriels des 60 derniers jours. L'administration de la Chambre fournit également des sacs de protection pour les appareils portables. Le Sénat a ses propres appareils et utilise les services de Services partagés Canada (« **SPC** »).

[18] M. Dicaire a signalé que son département n'a aucune autorité sur l'utilisation des ordinateurs personnels par les députés, mais offre plusieurs formations sur les types d'appareils électroniques qui peuvent être utilisés. Il fait remarquer qu'on ne peut pas savoir si un appareil personnel d'un député a été compromis à la suite d'une cyberattaque. Cependant, si un député soupçonne que l'un de ses appareils personnels a été piraté, celui-ci peut faire appel aux services informatiques de la Chambre en vue d'effectuer une analyse du contenu informatique.

[19] M. Dicaire a précisé que la protection des parlementaires s'applique aussi aux comptes informatiques. Il existe plusieurs moyens technologiques pour assurer la sécurité informatique des comptes, incluant l'authentification multifactorielle. Par ailleurs, il y a une politique en place qui interdit aux employés de la Chambre l'utilisation des comptes parlementaires sur les médias sociaux à des fins non-professionnelles.

[20] En cas de problème de cybersécurité, il existe un service disponible 24 heures sur 24, sept jours sur sept pour les parlementaires. La cybersécurité de la Chambre passe par les opérations de sécurité, le programme de sécurité, incluant la politique de sécurité, le respect des règles, la détection des menaces, ainsi que la sensibilisation et la formation du personnel.

[21] M. Dicaire a souligné qu'au cours d'une année donnée la Chambre est confrontée à un nombre faramineux de cyberattaques qui peuvent prendre plusieurs formes (ex., logiciels malveillants, hameçonnage, rançongiciel, Spamouflage, etc). La plupart du temps, les mécanismes de défense détectent et bloquent ce qui essaie de pénétrer dans le système, mais parfois, quelque chose réussit à passer. Dans ces cas, son équipe fait enquête et cherche à colmater les brèches dans le système. Il réaffirme que son mandat porte la continuité des opérations au Parlement.

[22] Lorsque les responsables de la sécurité des TI de la Chambre détectent une attaque, ils ne divulguent pas nécessairement qu'elle a eu lieu. Cela dépend des circonstances. Si une attaque vise un parlementaire en particulier, cette information lui est divulguée. S'ils doivent communiquer des informations relatives à une cyberattaque à des services de renseignement et de sécurité, le député concerné en est avisé. Mais en cas de cyberattaque infructueuse, ils ne préviennent personne. Le nombre de cyberattaques qui échouent est énorme.

[23] Le président de la Chambre est avisé d'une cyberattaque lorsque celle-ci a un impact sur les activités du Parlement ou pose un risque d'atteinte à la réputation de la Chambre.

4. Relationship with Government of Canada and others

4.1 Relationships with Government Departments, Agencies and Committees

[24] Commission Counsel asked about the relationship between HOC and the Government of Canada. Mr. McDonell explained that the Office of the Sergeant-at-Arms has memoranda of understanding ("**MOUs**") with CSIS and RCMP that provide for the exchange of information. He indicates that there is regular communication with both RCMP and CSIS. They also have MOUs with the Privy Council Office ("**PCO**"), including for the monitoring of cabinet meetings for bugs.

[25] The CIO has a MOU with the Communications Security Establishment ("**CSE**"), with whom there is a longstanding relationship. There are regular meetings with CSE, both scheduled and in response to specific incidents. The CSE's role has increased over the years, but today is focused on assisting with the protection of HOC infrastructure at the perimeter and assisting in incident management. There is also sharing of information between the CIO's team and the CSE relating to awareness, best practices and new trends. There are regularly scheduled meetings between the House and CSE, and some that are *ad hoc*, based on specific incidents. Mr. Dicaire described the partnership with CSE as a heathy collaboration.

[26] Mr. Dicaire indicated that HOC has an informal relationship with Shared Services Canada ("**SSC**") [SSC is the government institution responsible for providing unclassified digital services to Government of Canada organizations]. The House can use their services as needed, but is not required to. They are both part of a community of practices with other departments. He is invited to quarterly meetings at SSC.

[27] Mr. Dicaire further explained the HOC provides IT infrastructure for all parliamentary partners, including the Senate, Library of Parliament and PPS. The House and Senate IT teams work collaboratively on the same infrastructure.

[28] The Office of the Sergeant-at-Arms is a participant on INTERSECT, which is a community of first responders in the Ottawa region, which includes law enforcement, fire and emergency services. This body shares a variety of intelligence products with its members, including the HOC. There has been increased information sharing through INTERSECT since the 'Freedom Convoy' protests [in 2022].

[29] Mr. McDonell also sits on the Deputy Minister Protection Committee on ministerial protection. These meetings occur in a classified facility.

4.2 Information sharing between Government and HOC

[30] Mr. Dicaire explained that the circumstances in which he receives information from CSE respecting cyberthreats is quite formal. CSE generates technical bulletins pursuant to a formal protocol, with a request to action or a recommendation. Mr. Dicaire said that CSE is generally searching for "a piece of the puzzle". The information is 'Protected B' level and general or technical in nature. He described the information as being very rarely about people, and more often what an IP address is doing in relation to a particular network. CSE looks at the perimeter of HOC's IT infrastructure but has no visibility inside its network. CSE asks for help deciphering the information and Mr. Dicaire's team can provide assistance or visibility by investigating the technical information. Because the information provided by CSE is technical in nature, HOC does not know if the threat activity is generated by a foreign government or anyone else with an internet connection.

[31] Mr. Dicaire does not recall CSE ever speaking with him about a case of foreign interference. If they did, it was only in relation to technical information devoid of context, so he would not know that it was foreign interference related. The only time he recalls anything specific to foreign interference was during a briefing by CSIS.

[32] Commission Counsel inquired whether it would be helpful to receive contextual information from CSE. Mr. Dicaire said that it would. Some of the bulletins they receive contain unclear recommendations. Context could help to piece together the puzzle. He wondered however how effectively CSE could share that information. What is important is that the information shared allows the CIO to investigate the threat and ensure the HOC systems are stable. If more context information results in less technical information being shared due to security concerns, that would be an issue. Mr. Dicaire pointed out that the CIO and CSE have very different mandates: the CIO's primary duties are to protect parliamentary systems, ensure MPs have access to the network, and the network is not compromised to ensure that parliamentary business can continue. He does not have a national security mandate.

[33] Mr. McDonell explained that both his office and the RCMP generate reports every morning, Monday to Friday, regarding threats to MPs. The RCMP's reports have input from PCO Security and Intelligence. Both entities exchange their reports with one another, which provide updated threat information that has arisen over the previous 24 hours. On weekends, there are people available if something of concern occurs.

[34] The Sergeant-at-Arms and the RCMP jointly prepare threat assessments on all types of public activities and venues attended by MPs.

[35] The RCMP generates reports about demonstrations around the country, which are shared with the Sergeant-at-Arms. The SAA's OSINT also monitors and reports on demonstrations.

4.3 Security Clearances and Secure Facilities

[36] As MPs are elected by Canadians, they do not need a security clearance to sit in the House. Certain MPs may require one depending on a specific functions or

responsibilities they are performing. Such is the case for MPs performing certain ministerial or parliamentary secretary duties, or for MPs sitting on certain committees such as the National Security and Intelligence Committee of Parliamentarians ("**NSICOP**"). This responsibility falls to the government.

[37] The Speaker does not need a security clearance to perform his functions. However, the current Speaker, the Hon. Greg Fergus, has one because of his prior roles in Parliament.

[38] Both Messrs. McDonell and Dicaire have a top-secret security clearance. The office of the Sergeant-at-Arms has a number of employees with top secret security clearance based on the nature of their duties, which includes interacting with CSIS and RCMP.

[39] Mr. Dicaire also has a top-secret security clearance because he regularly meets with CSE. Some of Mr. Dicaire's analysts have a top-secret clearance due to the nature of their work.

[40] The House of Commons has a room on its premises where secret-level classified information can be exchanged, discussed and stored and another that can accommodate secret and top secret-level briefings. House Administration officials also attend off-site meetings in a sensitive compartmented information facility ("**SCIF**"). For Mr. Dicaire, these happen at CSE.

[41] Mr. McDonell indicated that there are currently plans to build a SCIF in the new Parliamentary Precinct as part of the current renovation work.

5. Security issues Related to MPs, Caucus, and Staff

5.1 Security issues related to MPs

[42] If there is a concern with an MP, they will communicate directly with the MP in question. There are direct lines of communication with MPs and often no need to go through a caucus or staff.

[43] Mr. McDonell explained that there are a variety of ways in which his office detects threats to MP's physical safety, which include through open-source intelligence, reporting from MPs and staffers, and through the RCMP or police of jurisdiction.

[44] Threats to physical safety are communicated directly to the MP. In some cases, the Sergeant-at-Arms will notify the whip or house leader of the MP's party. He will also notify RCMP and in particular cases PCO and security and intelligence agencies. Mr. McDonell points out that threats to, and harassment of, members happen every day.

[45] The House provides home security systems to MPs that are available both for their primary and secondary (i.e. national capital region) residences. Constituency offices can also be equipped with security systems.

[46] MPs and their spouses are provided with mobile duress alarms. In some more serious cases, security guards may be provided to protect an MP or their residence. MPs can request static, or fixed security for their homes or constituency offices. The Sergeant-at-Arms may also provide personal security details for Party Leaders. This is generally done on a case-by-case basis.

[47] The HOC administration has few security-related interactions with former MPs. There is an association of former MPs that has a small office within the Parliamentary precinct. The Sergeant-at-Arms has regular contact with this organization, but aside from issues related to building access privileges, there are essentially no security-related interactions with this group. Mr. McDonell could not recall any instances where a former MP was targeted by foreign interference that involved his office.

[48] Mr. Dicaire indicated that protecting former MPs from FI cyberthreats is not part of their mandate. If informed of such a threat, they would notify the relevant national agency. This has never happened thus far.

5.2 Security Screening of Members' Staff

[49] The office of the Sergeant-at-Arms is responsible for conducting security screenings of HOC personnel and staff. They conduct criminal background checks and perform 'loyalty to Canada' investigations with the assistance of the RCMP and CSIS.

[50] Loyalty to Canada investigations include a review of an individual's last five years of history. These investigations can be difficult, particularly if the candidate has resided outside the country, is new to Canada or is from a country that is of concern to Canada. Sergeant-at-Arms investigators may conduct 'resolution of doubt' interviews with candidates for employment. There has been a significant increase in the number of 'resolution of doubt' interviews conducted today as compared to what was done in 2019 or so; interviews are also more thorough than they once were. When the information submitted by the prospective employee is incomplete, his office wants to make sure they take the proper measures to protect their networks and their institutions. Most of the Sergeant-at-Arms' investigators are former police officer with extensive interview experience. The open-source intelligence unit gathers as much open-source material as possible on the prospective employee.

[51] The investigator conducting the 'resolution of doubt' interview makes a recommendation to the Sergeant-at-Arms to grant accreditation or not. The Sergeant-at-Arms has the final say. There is an informal appeal process in the event the prospective employer MP, who has discretion over whom they hire, disagrees with the Sergeant-at-Arms' decision not to grant accreditation. This generally involves the prospective employee contacting the Sergeant-at-Arms to appeal the decision. In one instance, the MP and the prospective employee met with the Sergeant-at-Arms.

[52] Mr. McDonell indicated that in the past ten years in his position, he has only refused a handful of accreditations over foreign interference concerns.

5.4 Security Concerns Related to Caucus and Caucus Staff

[53] In the case of concerns – security or other otherwise – relating to current caucus staffers, the Sergeant-at-Arms communicates with the Whip's office of the particular party.

[54] Some issues may be addressed with party whips or leaders, when the issue is of a more collective nature. Mr. McDonell indicated that in some cases it can be as informal as a hallway conversation.

[55] Asked whether HOC administration keeps contact with former MPs, Mr. McDonell indicated that they do, pointing out that there is a 'former parliamentarians association' that maintains a small office on the premises. The focus of the association is about transitioning MPs to post-Parliament life. He is in regular discussion with them. He has not yet had a case of a former MP bringing up concerns regarding foreign interference with his office. Former MPs maintain privileged access to Parliament Hill after their tenure.

6. Briefings for MPs and Staff respecting Foreign Interference

[56] House of Commons Administration coordinates with security, intelligence and law enforcement partners to provide unclassified briefings regarding foreign interference to MPs and staff. These briefings are developed by RCMP, CSIS, CSE and Public Safety Canada ("**PSC**"), who takes the lead. Briefings were provided over the past year to the various caucuses as a group, as well as to different sectors of HOC administration. These briefings relate to the current threat landscape and the precautions that can be taken.

[57] There are new positions within the office of the Sergeant-at-Arms related to security awareness. They focus more on briefing MPs on security, of which foreign interference is a big part. A focus of this briefing work will start with the next Parliament as part of the MP onboarding process. Briefings will touch on many subjects, including foreign interference.

[58] Mr. McDonell indicated that he wanted their security awareness program to be current at all times, and to brief members on an ongoing basis.

[59] Mr. Dicaire indicated that his office would do the same as relates to cybersecurity, as awareness is a big pillar of good cybersecurity. The foreign interference component in the cybersecurity briefings to MPs will be expanded.

[60] His team currently sends out cyber vigilance bulletins on current issues such as TikTok and phishing emails.

[61] Mr. McDonell indicated that these actions were not necessarily in response to recommendations made in the Procedure and House Affairs Committee ("**PROC**") report tabled in the House last year, noting that he had been advocating in favour of these types of briefings prior to that.

[62] When CSIS wants to meet an MP, the Sergeant-at-Arms and his office help coordinate and facilitate the meeting. They do not ask for specifics about why CSIS wishes to meet with the MP.

7. Dealing with misinformation and disinformation

[63] Commission Counsel asked whether mis and disinformation were in any way part of the House Administration's mandate of supporting MPs in their parliamentary functions. Mr. Dicaire noted that it was a topic they were more conscious about and increasingly monitoring, especially with the advent of AI and deepfakes. While the House Administration does not have a mandate to correct mis and disinformation and should not be seen as intervening in the political debate, there is a focus on building awareness and best practices. The HOC administration is careful not to intervene in political debate.

[64] There have been many cases of fake social media accounts impersonating MPs and fraudulent immigration websites using MPs' images. In this case, HOC will intervene with the platform operators and take steps to have the content taken down. They will generally get the authority from the concerned MP to act on their behalf, but this is not always necessary as the content generally violates the platform's terms and conditions.

[65] Mr. Dicaire described a PRC-linked "Spamouflage" campaign on social media targeting MPs' accounts that involved bots posting disinformation and propaganda in 2023. This campaign was brought to his attention by Global Affairs Canada ("**GAC**"). There was communication to MPs advising them of this particular campaign.

[66] The HOC administration does not engage with mis or disinformation related to the House itself. They instead attempt to position the House's website as the legitimate

source of information about the House. The biggest concern for Mr. Dicaire's team is the safeguarding of IT equipment and systems.

8. Specific incidents

8.1 The APT31 cyberattack targeting IPAC MPs

[67] Commission Counsel presented the interviewees with an unclassified document prepared by CSE outlining a chronology of events in relation to the APT31 email tracking link campaign in 2021 targeting MPs who were members of the Inter-Parliamentary Alliance on China ("**IPAC**"). Commission Counsel solicited their perspective on the chronology of events, more particularly to address the several instances in the report indicating that HOC IT Security was either unresponsive or did not provide feedback to requests by the Canadian Centre for Cyber Security ("**CCCS**").

[68] Mr. Dicaire indicated that the House IT services regularly receives reports from CCCS that are highly technical in nature. In this case, CCCS was seeking assistance on specific IP addresses. When the HOC receives such reports, they are required to acknowledge receipt as part of their protocol. In terms of the incident described in the report, only highly technical information was provided. There were vague recommendations on what to do, such as directing them to look at whether specific emails had reached people. CCCS only shared IP addresses. After investigating, HOC IT discovered that the emails in question did not reach their intended recipient and were quarantined by their security gateway. Therefore, there was no threat to Parliament or its infrastructure.

[69] Mr. Dicaire explained that they get a lot of reports like these. When they determine that there is no threat to parliamentary infrastructure, they do not do more. In this case, they reported back to CCCS on February 3, 2021 that the situation was "handled internally" because their system had handled it.

[70] The February 17, 2021 bullet indicates that HOC IT assessed that some MPs personal email addresses may have received the messages. Mr. Dicaire noted that personal email accounts were beyond HOC jurisdiction. The original information they received

related to MP IP addresses, which they assessed had not been compromised. He indicated that no contextual information was shared in the report received by CCCS, so they had no way of knowing whether this was a state-sponsored attack or otherwise. He noted that the source of a cyberattack did not make a difference from HOC's perspective, other than the fact that it is contextual information that could inform the HOC's understanding of the threat profile.

[71] Mr. Dicaire mentions that when they received the original report, the HOC did not yet understand that the emails in question were quarantined. They sent an email to all the eight MPs that were concerned inquiring whether they received emails from the domains in question. None of them responded that they had. Two MPs wrote back indicating that they would keep an eye out for them.

[72] Despite a request on February 24, 2021 by CCCS for copies of emails, HOC IT did not provide them as they did not have consent from MPs to do so. They did not seek consent, as the emails never reached their intended targets. That said, HOC IT provided CCCS with information, including metadata, about the emails on February 26, 2021. Mr. Dicaire drew a contrast with the Spamouflage campaign where there were concerns that emails might have reached targeted MPs. In that case, HOC IT worked with the Sergeant-at-Arms' office to obtain consent from members to go through their emails.

[73] In response to the March 17, 2021 bullet referring to an 8th report where CCCS asked the HOC IT security analyst for further technical or contextual information, Mr. Dicaire observed that if a request relates to a threat that was dismissed, it is possible they would not have responded because it was dealt with. He said that they would have told CCCS this, highlighting that the protocol between CCCS and HOC IT is very collaborative.

[74] Looking at the information contained in the report in question, Mr. Dicaire explained that CCCS asked them to investigate very specific and technical information. Responding to this type of request takes time as it requires a forensic analysis on the part of the HOC. In this case, the HOC's analysis indicated that the information CCCS was seeking related to a personal or guest device that was on HOC's guest network. Because the

device in question was not a HOC device, any threat to it did not constitute a threat to the parliamentary infrastructure. This information was, in fact, conveyed to the CCCS.

[75] Mr. Dicaire indicates that DSRP was not aware that the FBI informed the government in June 2022 that the activity referenced in the CCCS reports was related to a PRC-linked attack on parliamentarians who were members of IPAC.

[76] He explained that the HOC did receive a bulletin from the CCCS in June 2022 on the cyberattacks that the HOC had previously investigated. The bulletin did not mention APT31. Nor did it mention the FBI, with only reference made to a trusted partner. It mentioned only email addresses of individuals who are outspoken on topics relating to the Chinese Communist Party ("**CCP**") were targeted. The Bulletin related to technical details.

[77] Furthermore, the June 2022 bulletin referred to an attack in January 2022, not January 2021. Mr. Dicaire explained that HOC IT thought that the Bulletin was therefore referring to a different incident than the January 2021 issue. However, when the HOC IT investigated the issue, it could not locate any relevant information related to the date range cited by CCCS in the Bulletin. After notifying CCCS of this fact, CCCS corrected itself to state that the Bulletin should have referred to 2021, and not 2022.

[78] When the CCCS corrected the relevant dates, the HOC IT understood that the Bulletin related to the same 2021 issue that it had already addressed with the CCCS.

[79] The targeted MPs were not informed by the HOC administration in 2022 because the threat activity never reached them. CCCS also made no recommendation to advise them. Had HOC IT known that it was a state-sponsored campaign, they may have looked at it with a heightened sense of awareness for monitoring and business continuity purposes. But once they concluded that there was no actual threat, they did not brief anyone as per their usual practice.

8.2 The targeting of MP Michael Chong

[80] On the topic of reporting in 2023 indicating that MP Michael Chong received a briefing by CSIS that he was the target of an PRC interference campaign, the Sergeant-at-Arms

did not receive any intelligence products in relation to this incident and did not have specifics on the purpose of the meeting.

[81] The interviewees were not aware whether the HOC's input or feedback was sought prior to the enactment of the *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians* not long after this briefing. It informs them however that the threshold for informing MPs is lowered. Since the directive, there has been about the same frequency of information sharing, but there have been improvements in coordinating and communicating information to MPs. The Sergeant-at-Arms is a centralized point of contact.