

**Standing Committee on Government Operations and Estimates (OGGO)**  
**The subject matter of the launch, development, and maintenance of the ArriveCAN application**  
**November 14, 2022**

**QUESTION #1**

**MP Barrett:** Okay. I guess I would just ask who on appearing before us today, if they can identify themselves as being able to get to the information on **who can sign off on the waiving of security clearance and the potential implications of that, and if a threat assessment is done before, during or after that contractor has done work**, and if they can provide that information to the committee in writing because I imagine it will take a little bit of research. So I'm not sure, Mr. Chair, if we can just get someone from the witness panel to identify themselves that they'd be able to do that.

**Ms. Erin O'Gorman:** We'll get back to that information.

**RESPONSE #1**

All contractors were security cleared at time of issuance of the Task Authorization and before commencing any work.

The waiving of the requirement for security clearance in this case was related to the Request for Proposals bidding process. Government of Canada security offices were closed at the beginning of the pandemic, and therefore potential bidders asked whether resources could be proposed without that clearance in place. The response was that security clearance was not required at bid closing. However, Resource Evaluations and applicable security clearances were completed prior to any Task Authorization sign off and work commencing.

In addition, security was considered at every stage development of the ArriveCAN platform from design to implementation. The ArriveCAN solution inherits the security controls implemented on the CBSA Cloud platform and builds on them to implement application layer security controls. The key cloud platform security posture is implemented across five key security pillars:

- **Cloud Platform Security**
- **Identity and Access Management**
- **Network Security**
- **Cloud Security Governance Process**
- **Cloud Operations**

ArriveCAN included the following specific security measures:

- **Alignment to Specific GC and CBSA Policies** – Encryption of data at rest and in transit, API keys authentication for application level security.
- **Network Security** – All network connections traverse the Secure Cloud Enablement and Defence and CBSA perimeter network layers, network traffic logs sent to the Canadian Center for Cyber Security.

Annex 2 – Undertakings from the November 14<sup>th</sup> meeting

Annexe 2 – Engagements de la réunion du 14 novembre

- **Industry Security Best Practices** – Field validation to protect against standard web attacks, Apple/Google reviews prior to each implementation.
- **Vulnerability Testing and Analysis** – Vulnerability scanning, code review and static vulnerability analysis, vulnerability scans and penetration tests, formal review by the CBSA IT Security group.
- **Account Management** – Registration using verification code via email, user credentials follow GC standards for password complexity.
- **User Audits** – Cloud platform audit logging.

## QUESTION #2

**MP Johns:** [Inaudible] PSPC, if the 27 contracts disclosed by the CBSA were sole-sourced, in addition to a sole-sourced contract to KPMG by the Public Health Agency of Canada, given the number of sole-sourced contracts involved in this app, and the significant public attention on this issue, would you support a procurement practice review by the office of the procurement ombudsman?

**Ms. Erin O’Gorman:** I can take that. The last two and a half years

**MP Johns:** I just want to make sure it is specific to the review. I’m asking about the review.

**Ms. Erin O’Gorman:** — it’s very unique. We’re happy to learn lessons in whatever way we can, including the work that this committee is doing on ArriveCAN. We’re quite happy to have any lessons. The context in which the sole-sourced contracts were let was in the context of an emergency and insufficient time to have a competitive process.

**MP Johns:** Going back to one of my earlier questions around the initial estimated cost for the app: To be clear, I’m not asking about what was spent. We’ve heard that the preliminary development of the app was around \$80,000, and that the costs grew over time. I’m trying to find out whether those increases in cost were anticipated and, as the costs grew, was there an analysis done at each stage whether any of the work could be done in-house.

**The Chair:** I’m going to have to interrupt, because you are right on five minutes, Mr. Johns. However, if you could provide that to the committee in writing.

## RESPONSE #2

The costs for ArriveCAN were related to changes in public health measures at the border and so it was not possible to anticipate them when the app was initially developed in March-April 2020.

In terms of workforce, the ArriveCAN App was developed in-house, with existing CBSA employees and a mix of expert resources supplied by GC Strategies and a number of other companies. Overall, the CBSA’s Information Science and Technology Branch supports a 24/7/365 real-time border management environment, with 18,000 workstations, 180 enterprise applications, 5,000 mobile devices, 200 trace radiation detection and imaging units, all at over 400 ports of entry across Canada and international service locations worldwide – a significant demand to internal resources and staff. When the pandemic hit in March 2020, employees kept mission-critical systems running to ensure the continued flow of goods and essential travellers into the country. However, at the start of the pandemic, our experience with mobile technology and applications was still very limited and, recognizing this, CBSA required expertise from the private sector.

In general, staffing public service positions in mobile app development is extremely challenging as this expertise is in very high demand, including significant competition from the private sector. One of the CBSA’s strategies was to build integrated teams that enabled knowledge transfer from expert consulting resources to our staff, building out our employees’ skills and competencies over time. At each stage of development, the CBSA determined to what extent it was necessary to use external contracted resources. The result was that we used approximately 50 full-time equivalents across all ArriveCAN and ArriveCAN-related work, with a higher ratio of CBSA employees to professional service resources in the

Annex 2 – Undertakings from the November 14<sup>th</sup> meeting

Annexe 2 – Engagements de la réunion du 14 novembre

areas of IT Support, CBSA Systems, and Data Management where CBSA had the skills, experience, and capacity.

**Comité permanent des opérations gouvernementales et des prévisions budgétaires (OGGO)**

**Objet : lancement, conception et entretien de l'application ArriveCAN**

**14 novembre 2022**

**QUESTION N° 1**

**Député Barrett :** D'accord. Je suppose que j'aimerais simplement savoir si une des personnes qui comparaît devant nous aujourd'hui peut obtenir les renseignements suivants : **qui peut approuver une dérogation à la cote de sécurité? Quelles sont les répercussions potentielles d'une dérogation? Une évaluation de la menace est-elle effectuée avant le début des travaux, pendant les travaux ou après que l'entrepreneur ait terminé les travaux?** J'aimerais que ces renseignements soient fournis au Comité par écrit, car j'imagine qu'il faudra effectuer des recherches. Par conséquent, je ne suis pas certain, Monsieur le Président, si nous pouvons simplement demander à un des témoins de consentir à obtenir ces renseignements.

**Mme Erin O'Gorman :** Nous fournirons ces renseignements plus tard.

**RÉPONSE N° 1**

Tous les entrepreneurs ont fait l'objet d'un contrôle de sécurité lors de l'émission de l'autorisation des tâches et avant le début de tout travail.

La renonciation de l'exigence relative à la cote de sécurité, dans ce cas, concernant le processus de soumission de la demande de proposition. Les bureaux de la sécurité du gouvernement du Canada étaient fermés au début de la pandémie. Par conséquent, des soumissionnaires potentiels ont demandé s'il était possible de proposer des ressources sans cote de sécurité en place. On a répondu que la cote de sécurité n'était pas requise lors de la date de clôture de la demande de soumissions. Toutefois, les évaluations des ressources et l'obtention des cotes de sécurité applicables ont été effectuées avant l'approbation de l'autorisation des tâches et le début des travaux.

De plus, la sécurité a été prise en considération lors de la réalisation de la plateforme ArriveCAN, et ce, dès l'étape de la conception et tout au long de la mise en œuvre. La solution ArriveCAN hérite des contrôles de sécurité mis en œuvre sur la plateforme d'infonuagique de l'ASFC et les renforce en vue de mettre en œuvre des contrôles de sécurité de la couche application. La position de sécurité clé de la plateforme d'infonuagique est mise en œuvre à l'échelle de cinq piliers en matière de sécurité :

- **Sécurité de la plateforme infonuagique**
- **Gestion de l'identité et des accès**
- **Sécurité du réseau.**
- **Processus de gouvernance de la sécurité du nuage**
- **Opérations infonuagiques**

Annex 2 – Undertakings from the November 14<sup>th</sup> meeting

Annexe 2 – Engagements de la réunion du 14 novembre

ArriveCAN comprenait les mesures de sécurité qui suivent :

- **Harmonisation avec des politiques propres au GCet à l'ASFC** – chiffrement des données au repos et en transit, authentification par clé API pour la sécurité à l'échelle de l'application.
- **Sécurité du réseau** – toutes les connexions réseau traversent l'activation et de défense du nuage sécurisé et les couches de réseau périmétriques de l'ASFC, les journaux de trafic dans le réseau sont envoyés au Centre canadien pour la cybersécurité.
- **Pratiques exemplaires de l'industrie en matière de sécurité** – validation des champs pour empêcher les attaques Web standard, examens d'Apple/de Google avant chaque mise en œuvre.
- **Tests et analyses de vulnérabilité** – analyse de vulnérabilité, examen du code et analyse des vulnérabilités statiques, analyses de vulnérabilité et tests de pénétration, examen officiel par le groupe de la sécurité des TI de l'ASFC.
- **Gestion du compte** – inscription au moyen d'un code de vérification envoyé par courriel, les identifiants d'utilisateur satisfont aux normes du gouvernement du Canada en ce qui concerne la complexité des mots de passe.
- **Vérification des utilisateurs** – utilisation de journaux de la plateforme d'infonuagique.

## QUESTION N° 2

**Député Johns** : [inaudible] SPAC, si les 27 contrats divulgués par l'ASFC ont été accordés à un fournisseur unique, en plus d'un contrat accordé à un fournisseur unique à KPMG par l'Agence de la santé publique du Canada, compte tenu du nombre de contrats accordés à un fournisseur unique lié à cette application, et en raison de l'attention du public considérable concernant cette question, comment appuieriez-vous un examen des pratiques d'approvisionnement par le Bureau de l'ombudsman de l'approvisionnement?

**Mme Erin O'Gorman** : Je pourrais m'en occuper. Au cours des deux dernières années et demie

**Député Johns** : Je veux simplement m'assurer que cela concerne uniquement l'examen. Ma question concerne l'examen.

**Mme Erin O'Gorman** : — C'est très unique. Nous sommes heureux de tirer des leçons de toute façon qui soit, y compris grâce au travail sur ArriveCAN effectué par le Comité. Nous sommes très heureux de tirer des leçons. Les contrats accordés à un fournisseur unique ont été permis, car il s'agissait d'une urgence et qu'on n'avait pas suffisamment de temps pour effectuer un processus concurrentiel.

**Député Johns** : Pour donner suite à une de mes questions antérieures sur le coût estimatif initial de l'application et pour être clair, je ne veux pas savoir ce qui a été dépensé. Nous avons entendu que la conception préliminaire de l'application a coûté environ 80 000 \$ et que les coûts ont augmenté au fil du temps. Je tente de déterminer si ces augmentations des coûts étaient prévues et, lorsque les coûts augmentaient, si une analyse a été effectuée à chaque étape afin de déterminer si des travaux pourraient être faits à l'interne.

**Le président** : Je vais devoir vous interrompre, parce que vous avez atteint cinq minutes, M. Johns. Toutefois, vous pourriez fournir ces renseignements au Comité par écrit.

## RÉPONSE N° 2

Les coûts d'ArriveCAN découlaient de la modification des mesures frontalières de santé publique; il n'était donc pas possible d'anticiper ces coûts lors du développement initial de l'application en mars et avril 2020.

En termes de personnel, l'application ArriveCAN a été conçue à l'interne par nos employés, de même que par un ensemble de ressources expertes provenant de GC Strategies et d'un certain nombre d'autres entreprises. Dans l'ensemble, la Direction générale de l'information, des sciences et de la technologie de l'ASFC appuie un environnement de gestion frontalière en temps réel et en tout temps comptant 18 000 postes de travail, 180 applications organisationnelles, 5 000 appareils mobiles, 200 appareils de détection de trace de rayonnement ou d'imagerie dans plus de 400 points d'entrée au Canada et points de service à l'étranger - une demande importante pour les ressources internes et le personnel. Lorsque la pandémie est survenue, en mars 2020, les employés devaient s'assurer que les systèmes essentiels à la mission étaient en bon état de fonctionnement pour veiller à la bonne circulation des biens et des voyageurs essentiels au Canada. Cependant, au début de la pandémie, notre

## Annex 2 – Undertakings from the November 14<sup>th</sup> meeting

## Annexe 2 – Engagements de la réunion du 14 novembre

expérience de la technologie et des applications mobiles était encore très limitée et, reconnaissant cela, l'ASFC avait besoin de l'expertise du secteur privé.

En général, le recrutement dans le secteur public de spécialistes de la conception d'applications mobiles est extrêmement difficile, car cette expertise est très prisée, y compris une concurrence importante du secteur privé. Une de nos stratégies consiste à mettre sur pied des équipes qui permettent d'échanger des connaissances d'experts-conseils à nos employés afin d'aider à perfectionner les compétences de nos employés au fil du temps. À chaque étape de développement, l'ASFC a déterminé dans quelle mesure il était nécessaire d'utiliser des ressources contractuelles externes. Le résultat a été que nous avons utilisé environ 50 équivalents temps plein pour tous les travaux liés à ArriveCAN, avec un ratio plus élevé d'employés de l'ASFC par rapport aux ressources de services professionnels dans les domaines du soutien informatique, des systèmes de l'ASFC et de la gestion des données où l'ASFC possédait les compétences, expérience, et une capacité.