

COMMISSAIRE AUX ÉLECTIONS FÉDÉRALES



COMMISSIONER OF CANADA ELECTIONS

MEMORANDUM

Protected A

DATE: May 23, 2024

TO: Caroline J. Simard

C.C.: Brahim Achtoutal, Mylène Gigou, **OCCE** [REDACTED]

FROM: Carmen Boucher

REF.: Virtual Meet & Greet with the Chief of Communications Security Establishment

BACKGROUND

- There is no memorandum of understanding (MOU) between the OCCE and CSE.
- Since 2019, our office has engaged with CSE in preparation for both the 2019 and 2021 federal general elections on the topic of cyber threats to Canada's democratic process. Although our communication with CSE has been more limited than perhaps other SITE members communication channels are open.
- CSE, and in particular the Canadian Cyber Centre (CCCS often called "triple-C-S") is responsible for protecting government infrastructure and providing advice to government entities in this regard. As our Information Technology (IT) infrastructure is provided, maintained and protected by Elections Canada (EC), the relationship in this regard is between EC and CSE
- CSE is a core member of SITE, and the Elections Security Coordination Committees (ESCC) and as such there is often joint participation between our two organizations in this forum.

CONSIDERATIONS

- The RCMP [REDACTED] provides OCCE with support for analysis of technical products, [REDACTED] search warrant to audio or visual content collected in various manners during a review or investigation. [REDACTED] CSE supports the RCMP in its technical efforts, including in providing technical advice, technical tools, decryption and support for attribution of origin.
- The CSE does not have a mandate to directly support the OCCE in a similar manner, and as such, this type of support would be indirect, as CSE would support the RCMP AVAU.

Operational Avenues

SCIF Access

Our current access to classified products continues to be paper only, via CSIS. Our goal is to have electronic access to the distribution system, which is managed by CSE [REDACTED]

We have identified a [REDACTED] for access at [REDACTED] and they are willing to enter into a co-use agreement with us. In order to do so, we need to become an Authorized Organization (AO), and select staff will need to receive the appropriate indoctrinations, including for SIGINT.

[REDACTED] has offered to provide access to their TS SCIF and to access their CTSN terminals within the SCIF upon approval of a SCIF Co-Use Agreement. However, this agreement must be signed by both a Compartment Information Control Officer (COMCO) & an Information Systems Security Officer (ISSO), two positions that neither EC nor the OCCE have. Access to the SCIF also requires additional indoctrinations, and at present there is no internal ability to indoctrinate employees. AO status would enable these organizations to independently implement and maintain the necessary indoctrinations, and the continued compliance and maintenance of SCIF physical security measures to securely receive, process and store classified materials.

Status: The memo is in final draft and will need to be signed by CCE and **Elections Canada**, as Chief Security Officer. The memo is addressed to **CSE** [REDACTED] at CSE. Goal is for internal approvals to be obtained for mid June.

Request for CSE:

It would be appreciated if CSE can request that the AO request be prioritized by CSE upon receipt. The goal is obtain access to a SCIF prior to the next election, and as noted above, there are several steps towards this. The AO is the necessary approval for other processes to commence.

Indoctrinations

We have inquired about indoctrinations for select staff for SI content, via **CSE** [REDACTED] who attends as CSE rep on the SITE TF. So far no progress and we are following up with CSE via EC Enterprise Security. No need to actively address with Xavier, but in the event it is raised or relevant. Indoctrinations are needed for classified meetings, classified reporting, and access to SCIF facilities and CTSN.

Interpreter Support

We are looking to build a list of cleared contractors for oral interpretation in select languages. Would CSE be able to provide names or referrals of individuals who may be able to provide ad hoc interpretation for interviews? We are approaching CSIS with the same request.

NEXT STEPS

- Your Office has coordinated the contact with Ms. Xavier for the 29 of May, 2024.
- A memo is being drafted by EC Enterprise Security will be submitted to you and [REDACTED] for your respective approvals circa mid-June, 2024, which would provide authorization to engage with a request to CSE for AO Status. EC will be lead in this engagement, while the Executive Director, Enforcement, actively supports these efforts.
- Should AO status be granted, individuals within EC will need training from CSE in order to meet the requirements for SCIF access. OCCE staff will need to be provided with the requisite indoctrinations and software training, prior to obtaining autonomous S CIF access.

