ADM: Patrice Nadeau (613) 688-9263
DG: Giselle Marasco (613) 978-0034
SDir : Vincent Chouinard-Prevost (613) 294-4668

Security: **PROTECTED B**

**MEMORANDUM TO THE SENIOR DIRECTOR**

**FOR INFORMATION**

## SUBJECT

Decryption as Mandatory or Optional for Partner Onboarding Secure Cloud Enablement and Defence (SCED)

SUMMARY

This memorandum is to provide the background and guidance pertaining to decryption as mandatory or optional for Partner onboarding. Decryption at the Secure Cloud Enablement and Defence (SCED) layer has not been communicated as mandatory. An analysis was requested to be conducted in order to provide guidance on decryption being mandatory or optional. A review of the supporting documents clearly demonstrates that the enablement of decryption, as part of the SCED service is mandatory across subscribed clients, with a defined process for exemptions. This exemption process is at the discretion of Shared Services Canada (SSC).
Recommendation: Inform the Tripartite stakeholders of the decryption supporting documentation.

## BACKGROUND

A first Treasury Board Submission (Workload Migration and Cloud Enablement in support of Budget 2018 Measure – “Enabling Digital Services to Canadians”) provides the basis of this decryption analysis, in addition to a follow up TB submission in September 2020.

The September 2020 SCED Treasury Board Submission Section 22.
22. SCED’s security function is accomplished through a combination of virtual and physical security controls that are designed to block harmful content, and through continuous monitoring and scanning of the environment. With that in mind, the components of the pilot are explained as follows:

- Testing a “physical” security infrastructure at a co-location facility. This infrastructure forms security controls by way of a multi-functional security infrastructure (**decryption**, inspection, firewalling, malware detection and intrusion detection and prevention), at the point where the GC enterprise

connects with the external network and enables the connectivity to the CSP. It facilitates secure communication pathways between GC data centres and cloud-based infrastructure that is hosting government information and assets.

Based on section 22, bullet 2, the wording provides support for SCED decryption being mandatory.

Concept of Operations (signed) August 27, 2020, Page 74.

**SSL/TLS DECRYPTION**

**The SSL/TLS Decryption is required** to ensure that encrypted traffic does not contain intrusion attempts or possible malware.

**The SSL/TLS Decryption device will decrypt** the traffic and then pass the traffic to the IDPS which will analyze the data stream against specific policies, whitelists/blacklists and other intelligence gathered by SSC from users of the service and vendors of the security GC-CAP virtual security stack. **Both egress and ingress SSL/TLS encrypted traffic will be decrypted**, analyzed, re-encrypted and then sent to their final destination. Controls will be in place to address exception requests. The security functions will be transparent to the user.

SSL/TLS encrypted transmissions will be selected for decryption, analysis and re-encryption based on the partner department and agency requirements before they can be forwarded to their destination. **Exceptions to this rule will need to be justified and presented to Security Management for consideration**. For example, if a partner department or agency decides to use this portion of the service but **wishes to exclude its SSL/TLS transmissions from scrutiny by the SCED system, then the partner department will need to complete an exception request and submit it to the SSC SOC for consideration**.

**KEY CONSIDERATIONS**

SSC has onboarded  multiple Partners without decryption being enabled as a mandatory requirement. A communications strategy will need to be developed to present partners with decryption as a core piece of any subscription to the SCED service.

**NEXT STEPS**

Information on the supporting documentation to be communicated to the Tripartite and the Chief Technology Branch (CTOB)  in order to develop a next steps strategy.

**RECOMMENDATION**

Inform the Tripartite stakeholders and provide awareness on the decryption supporting documentation. Communicate with the CTOB in order to raise awareness to clients about the requirement to decrypt their SCED related traffic.

**References/documents reviewed:**

- **Canada's Cyber Security Strategy**
- **Treasury Board Secretariat SCED TB Submission September 2020**
- **SCED Implementation Business Case**
- **SCED Project Brief**
- **SCED Project Management Plan**
- **SCED Project Charter**
- **SCED Concept of Operations**