STATEMENT TO ESTIMATES SPILOVER HEARING

Thursday 14 November 2019

I wish to update Senators in relation to the cyber security incident that impacted the parliamentary network earlier this year.

I have been asked about how the incident affecting the network was executed. While I do not propose to discuss operational security matters in detail, I can state that a small number of users visited a legitimate external website that had been compromised. This caused malware to be injected into the parliamentary computing network.

I reveal this information as a salient warning to all users of the parliamentary network that they must be cautious and vigilant when clicking on any documents, attachments or links that are outside of our environment.

I have been asked if there was any insider involvement or assistance in the compromise and I can confirm there is no evidence of an insider threat.

The Department of Parliamentary Services (DPS) became aware of the incident on the 31 January 2019. DPS and the ASD acted immediately to monitor activity and plan an effective remediation. Removal of the attacker occurred on the 8 February 2019.

I've advised previously that a small amount of non-sensitive data was taken from the network. While we cannot precisely guarantee that no other data was removed, extensive investigation has provided no evidence of this.

The small amount of non-sensitive data refers to DPS corporate data and data related to a small number of parliamentarians. Discussions either have or will occur with the affected offices. I can advise that two Senators were contacted at the time, as soon as the breach was identified.

I have also been asked whether any law enforcement or intelligence agencies had access to the parliamentary system during the investigation and whether this access was supervised. DPS and the Australian Signals Directorate (ASD) worked side by side in a collaborative manner in the investigation and remediation of the cyber incident. All ASD access was approved by and advised to DPS. ASD access related to investigating technical systems, logs, scanning network traffic, identifying malware and other vulnerabilities.

Neither ASD nor DPS accessed data or information stores held by parliamentarians without their consent. These technical investigations do not access the contents of parliamentarian's documents, emails or communications and are limited to information required to diagnose and remediate cyber incidents.