Senate Finance and Public Administration Legislation Committee —Additional Estimates Hearing—February 2012

Answers to Questions on Notice

Parliamentary departments, Department of Parliamentary Services

Topic:	**CCTV cameras**
Question:	**45**
Hansard reference	**Written**

Date set by the committee for the return of answer: 30 March 2012

1. Mr Hallett notes that while the President must approve access to footage, it is possible to do so without consent. Is a system 'log' kept of all users who access the footage?
2. Do all DPS staff have access to security footage?
3. In their response to Question 15 (Supp Estimates 2011), the Department stated that 'Control room operators have been reminded of the importance of reporting instances of workstation reboots, so that issues can be diagnosed and resolved'. Does the DPS monitor system reboots by security camera operators? If a reboot is not reported, has the DPS any way to detect this?
4. With respect to the 'isolation' of the security cameras from the wider network, could a computer crash caused by a virus or multiple server outages in the Parliamentary Computer Network result in parliament house security cameras failing? What contingency plans are in place to deal with that possibility?

Answer

1. No. A system log is not kept to record which cameras are being displayed. Only a small number of staff in the security section have access to the CCTV system. A CCTV Code of Practice has been established and endorsed by the Presiding Officers to protect sensitive and privileged CCTV imagery. The CCTV Code of Practice is publicly available on the Parliament House website. Staff who have access to this system occupy a position of trust within DPS and are required to have a valid national level security clearance. These staff are also required to formally acknowledge and agree to comply with the requirements of the CCTV Code of Practice.

2. No.

3. Yes. As part of the CCTV system maintenance period, DPS is monitoring issues that require workstation and server reboots. Workstation reboots are monitored through reports by individual operators. Server reboots are monitored through system logs.

4. As advised previously, a server crash will result in lost CCTV capability. Contingency plans include the use of Australian Federal Police, Parliamentary Security Service officers and security systems such as sensors, alarms and secure radio networks.