Question: BET 558

Topic: **Protective Security Policy Framework**

Written: **17 June 2013**

Senator BUSHBY asked:

558.   Provide an update for your department/agency, including what is your current compliance level, what are you doing to manage risk, what is being done to comply with the mandatory requirements and details of any department/agency specific policies and procedures.

Answer:

What is our current compliance level?

ASIC is fully compliant with 24 of the 33 PSPF mandatory requirements and partially compliant with the remaining requirements. It expects to be fully compliant with 31 of the mandatory requirements by 31 July and partially compliant with the remaining two given the recent changes to the Information Security Manual (ISM) in April 2013.

What are we doing to manage risk?

Risk is being managed within the PSPF project and is overseen by the project board and ASIC's Risk Committee and the Commission.

What is being done to comply with the mandatory requirements?

A PSPF Steering Committee has been established, which includes key business representatives. The Committee meets on a regular basis to focus on establishing compliant policy documentation, developing supporting structures, communicating changes to staff and ensuring ASIC has measures in place to comply with our security obligations.

Details of any department/agency specific policies and procedures

The Commission approved:

 (1) ASIC's security policy framework and attendant security policies covering information, personnel and physical security on 22 August 2012;
 (2) ASIC's Fraud Control Policy and Framework on 30 January 2013 and launched the policy, framework and mandatory online training module on 20 February 2013;
 (3) The launch of general security awareness and new security induction mandatory online training modules on 6 May 2013; and the launched of the new mandatory online information security training module on 10 June 2013.

Since 1 March 2013, the PSPF Steering Committee approved twenty (20) security protocols, two (2) security plans, two (2) security manuals and eight (8) employees guides covering information, personnel and physical security requirements as well as subjects covering reporting of security incidents, outsourcing, working away from the office and event security.