AGENCY/DEPARTMENT: DEPARTMENT OF INDUSTRY, INNOVATION, SCIENCE, RESEARCH AND TERTIARY EDUCATION

TOPIC: Protective Security Policy Framework

REFERENCE: Written Question - Senator Bushby

QUESTION No.: SI-119

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

The Department is working through all 33 mandatory requirements of the new Protective Security Policy Framework and a compliance framework has been developed to enable the Department to achieve full compliance. The Department is moderately compliant and progress reports are provided quarterly to the Department's Executive Security Committee. For this Department a moderate level of compliance recognises that the majority of the documentation required for PSPF reporting is already established. However, due to offices relocating and amalgamating as part of the Machinery of Government change (the majority of these offices will be relocated prior to the end of June 2013) we currently anticipate we will not be fully compliant until the first reporting period of July/August 2013.

The new email classification system has been successfully rolled out within the Department.

In managing risk, the Departmental risk assessment is updated twice yearly. Security risks are included in this assessment and new security upgrade work is currently being undertaken across the Department.

Departmental policies and procedures such as Agency security plans, updating business continuity plans and staff security awareness training are all in the process of being updated to reflect the new requirements.

Specific Departmental policies are being updated and/or developed on the following:

- Physical security
- Information Security
- Information Technology Security.

In addition, a number of Departmental procedures are being updated and/or developed, including in the following areas:

- Guidance on home-based work.
- VIP/Event security.
- Dealing with the media.
- Protocols for Managing Australian Federal Police Requests for Information.
- Actions to be undertaken if the Australian Government Terrorism Public Alert Level is raised or in the event of demonstration or protest activity.
- Identity Cards/Access Control.
- What is 'security classified' information and 'sensitive' information.
- Staff security awareness training.