Senate Economics Legislation Committee
ANSWERS TO QUESTIONS ON NOTICE
Industry, Innovation, Science, Research and Tertiary Education Portfolio
Additional Estimates Hearing 2012-13
13 February 2013

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

TOPIC: Protective Security Policy Framework

REFERENCE: Written Question - Senator Bushby

QUESTION No.: AI-151

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

DEPARTMENT OF INDUSTRY, INNOVATION, SCIENCE, RESEARCH AND TERTIARY EDUCATION

The department is working through all 33 mandatory requirements of the new Protective Security Policy Framework (PSPF) 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 the 2011 Machinery of Government change and a recent internal relocation project, some PSPF requirements may not be met for the first reporting period. The department is planning for property alignment by 2013-14 and expects to be fully PSPF compliant by this time.

AUSTRALIAN INSTITUTE OF ABORIGINAL AND TORRES STRAIT ISLANDER STUDIES (AIATSIS)

As a *Commonwealth Authorities and Companies Act 1997* agency, AIATSIS is not required to comply with the PSPF.

Regardless, AIATSIS have engaged the service of the Australian Federal Police (AFP) consultancy service, to evaluate AIATSIS's level of compliance, risk exposure, and to provide a plan to enhance and manage risk and deliver training sessions to staff.

A report was provided to the department in January 2013 for a consolidated response.

AUSTRALIAN INSTITUTE OF MARINE SCIENCE (AIMS)

As a *Commonwealth Authorities and Companies Act 1997* agency, AIMS is not required to comply with the Protective Security Policy Framework.

However, AIMS management is strongly committed to security matters and has implemented a risk based approach to ensure fit-for-purpose implementation of security measures. AIMS is currently reviewing these against the 33 mandatory requirements of the Protective Security Policy Framework. The initial review indicates that there is already a high level of compliance. For example, AIMS has a comprehensive security system in place to protect its people and its scientific infrastructure. This includes access control, security cameras and after hours security presence.

AUSTRALIAN NUCLEAR SCIENCE AND TECHNOLOGY ORGANISATION (ANSTO)

As a *Commonwealth Authorities and Companies Act 1997* agency, ANSTO is not required to comply with the PSPF.

Nevertheless, ANSTO has a comprehensive security system in place to protect its landmark scientific infrastructure. This system includes 24 hour a day protection by the AFP and controlled access to the site through an AFP checkpoint with photo identification and security cameras.

ANSTO also meets all international requirements for security including those set by the International Atomic Energy Agency (IAEA), the world's centre of cooperation in the nuclear field.

According to the Nuclear Materials Security Index, released by an independent organisation in 2012, Australia has the best nuclear materials security in the world.

In addition to its physical protection measures, ANSTO has a vast array of other hard and soft security measures and initiatives in place including:

- restricted access to sensitive areas, such as Australia's only research reactor, OPAL. Access is determined by the independent nuclear regulator, the Australian Radiation Protection and Nuclear Safety Agency (APANSA);
- regular emergency training and preparedness training exercises held in collaboration with other state and federal government emergency response agencies;
- security training as part of the staff induction process;
- security checks on all staff and contractors;
- compulsory ongoing security awareness training for all staff; and
- regular checks and audits.

AUSTRALIAN RESEARCH COUNCIL (ARC)

ARC has implemented the new eMail protective marking requirements as part of the Agency desktop Standard Operating Environment (SOE). The Agency Strategic Risk resister is managed and maintained under the guidance of the Senior Management Group which includes Agency Security risks. Agency security plans for Physical and Information Security are maintained and managed by the appropriate Agency Security Adviser and IT Security Adviser.

AUSTRALIAN SKILLS QUALITY AUTHORITY (ASQA)

ASQA is currently not fully compliant with the PSPF, but as an agency in its second year of operation ASQA has made significant progress toward full compliance.

ASQA is working through all 33 mandatory requirements of the new Protective Security Policy Framework and a compliance framework and implementation plan have been developed to enable ASQA to achieve full compliance as soon as practicable.

ASQA has an approved Agency Security Policy, Business Continuity Plan, Fraud Control plan, IT security policy, while the ASQA IT environment is managed by the Department of Education, Employment and Workplace Relations (DEEWR) and is subject to DEEWR's security and access controls.

COMMONWEALTH SCIENTIFIC AND INDUSTRIAL RESEARCH ORGANISATION (CSIRO)

As a *Commonwealth Authorities and Companies Act 1997* agency, CSIRO is not required to comply with the PSPF.

Regardless, the CSIRO is currently working through all 33 mandatory requirements of the PSPFand a framework has been developed to enable full compliance. The CSIRO is moderately compliant and progress reports are provided quarterly to the CSIRO’s Security Committee. The CSIRO anticipates it will be 92 per cent compliant by the first reporting period of July/August 2013.

The key strategies being employed to establish a robust organisational security posture are:

- understand organisational security threat and risk;
- engaging with Division/Flagship Directors to contextualise security risk and compliance commensurate with, business objectives, key alliances, partnerships and collaborators and critical assets;
- ensure security seamlessly integrates into business line processes – prevention, compliance, reporting and performance;
- greater accessibility to and promotion of staff education, awareness and aftercare programs through mechanisms such as a Security eLearning module; and introducing staff accountability measures; and
- rationalise and ‘position base’ security clearance requirements across the organization.

In managing risk, the CSIRO risk assessment is updated annually. Security risks are included in this assessment and new security upgrade work is currently being undertaken across the organisation.

The CSIRO policies and procedures such as the CSIRO 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 organisational policies are being updated and/or developed for the following:

- physical security;
- information security; and
- information technology security.

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

- Guidance on home-based work.
- VIP/Event security.
- Dealing with the media.
- Identity Cards/Access Control.
- What is 'security classified' information and 'sensitive' information.
- Staff security awareness training.

IP AUSTRALIA

IP Australia has made considerable progress against all 33 mandatory requirements of the new PSPF. This is further consolidating protective security works and policy development following on from security reviews conducted by the AFP in 2009 and 2011.

A six monthly report is provided to the Director General and Executive by the Agency Security Adviser outlining IP Australia's progress against the 33 mandatory requirements of the PSPF. The first report was tabled in September 2011. IP Australia is moderately compliant with the 33 mandatory requirements of the PSPF.

IP Australia has sought assistance from the AFP in relation to security risks faced by the agency. This supplements our own risk management policies and procedures.

Formal security risk reviews have been conducted covering personnel security to meet a PSPF requirement, overall IP Australia compliance with PSPF requirements and protection of sensitive IP Australia material/patents for example. Recommendations from these reviews have been considered and implemented as necessary.

In addition, internal security policy and procedures including IP Australia's Chief Executive Instructions are being updated to reflect the current requirements of the PSPF.

A number of new PSPF compliant policies have been developed and/or existing security policies updated to reflect new requirements including a personnel security policy and waiver of nationality policy for example.

The new email security classification system has been rolled out at IP Australia.

TERTIARY EDUCATION QUALITY AND STANDARDS AGENCY (TEQSA)

TEQSA is implementing the 33 mandatory requirements of the PSPF and aims to achieve compliance by the end of the financial year. Under the four sections of Governance, Personnel, Information and Physical security, TEQSA has developed and/or implemented 29 of the requirements. The remaining four are currently under development and aim to be finalised by the end of the financial year.

TEQSA has established a Security Committee which meets (at a minimum) twice per calendar year and an Audit Committee which meets four times per calendar year.

In 2012, TEQSA implemented an Enterprise Risk Management Framework (ERMF) and contemporary methodology (ISO31000:2009) for identification, management and controls of risks to the agency.

Specific training programs are developed with the agency commencing delivery to all staff and implementation into the formal induction program. These include Fraud Awareness, Security Essentials and Risk Management Fundamentals training.

Specific policies and procedures include:

- TEQSA ICT Security User Policy
- TEQSA Agency Classification Guide
- TEQSA Enterprise Risk Register
- TEQSA Risk Appetite Statement
- TEQSA Risk Management Communique #1
- Security Essentials training package
- Fraud Awareness training package
- Risk Management Fundamentals training package
- Applying Risk Management Principles training package
- TEQSA Fraud Control Plan
- TEQSA Agency Security Plan
- Designated Security Assessed Positions register
- TEQSA Business Impact Assessment
- Working From Home Policy (management of associated risks).

TEQSA will work with the department regarding the actions required if the public alert/threat level is increased by the Commonwealth.