Attachment 1

Australian Government

Department of Foreign Affairs and Trade

REPORT TO THE JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

REPORT No. 471

Inquiry based on Auditor-General's Report No.5 (2017-18)

Please note: DFAT has submitted additional information to the Committee which contextualises aspects of this report.

Response to the recommendation(s)

Recommendation No. 1

That DFAT make available to the Committee:

(i) an extract of the findings and recommendations from the internal audit of the Departmental Security Framework (to be undertaken in 2018), and an outline of how DFAT intends to address these

(ii) a summary of how the Framework addresses the key issues identified in this report, giving particular emphasis to the matters raised in paragraph 2.3

DFAT's Internal Audit Branch commenced a two-part audit into the implementation of the DFAT Security Framework (DSF) on 23 August 2018. Part One of the audit was completed on 25 October. The objective of Part One was to "provide assurance to the Audit and Risk Committee (ARC) that the DSF had been implemented:

- with a clear communication and outreach strategy
- using appropriate communication to DFAT staff, including highlighting key changes, and
- with training, advice and support to DFAT staff".

Part Two, which will take place in March-April 2019, will focus on the implementation of the new risk assessment and reporting requirements for posts under the DSF.

The DSF, which was launched in March 2018, addresses the key issues identified in the Joint Committee of Public Accounts and Audit (JCPAA) report No.471, and in particular paragraph 2.3, in three ways.

First, the DSF outlines security roles and responsibilities and also notes the level of risk delegation for each of those positions. The Security Branches have conducted a significant amount of outreach in 2017 and 2018 to ensure familiarity with the DSF by security leaders.

Second, it establishes a baseline for assessing security risks in Australia and at overseas missions through the development of a set of Security Risk Assessment (SRA) tools. The DSF SRA tools comprise a likelihood scale, a consequence scale, a risk matrix and a risk delegation matrix. To support this, the DSF also provides standard templates for developing risk mitigation strategies and risk registers.

Third, it establishes a new stream of policy and procedures on security assurance. The DSF defines how the Security Branches will deliver key functions, such as security inspections and investigations. It outlines a range of new reporting requirements for posts, which give greater levels of assurance regarding the security risks being managed at post. This reporting helps to inform and prioritise the operational work of the Security Branches. The assurance policy stream also details DFAT's approach to non-compliance through a new breach policy.

The Security Branches have linked their performance to the effective implementation of the DSF as outlined in its Strategic Plan, Business Plan and DFAT's Corporate Plan.

Recommendation No. 2

That DFAT reports on its progress in implementing recommendations from:

(i) the Review of Diplomatic Security (May2015)

(ii) Auditor-General's Report No.5 (2017–18), complete with timeframes, planned deliverables and outcomes observed to date

All of the recommendations from the Review of Diplomatic Security (May 2015) have been addressed.

Six of the nine ANAO Audit Report recommendations have been implemented as part of a dedicated Continuous Improvement Project. Implementation of recommendations 2(a), 6 and 7 will occur through a Security Enhancements Program that has been established following the allocation of funding under the Mid-Year Economic and Fiscal Outlook (MYEFO) 2018-2019.

Recommendation No. 3

That DFAT assess whether current independent assurance arrangements provide sufficient and ongoing oversight of its overseas security management, and take timely action accordingly

DFAT's current independent assurance arrangements comprise principally of audits, reviews, reporting and governance committees. DFAT considers that these provide sufficient and ongoing oversight of its overseas security management. However, it recognises the value of strengthening independent oversight and has appointed an external member to the new Operations Committee. This committee, which replaces the Departmental Security Committee, is charged with overseeing the department's key risk management systems, including security.

Several audits and reviews were undertaken in 2018 to provide assurance and oversight. A number of independent cultural reviews have also been commissioned to address specific security concerns.

DFAT is satisfied with the assurance these audits/reviews provide. Each audit/review has identified room for improvement in the management of overseas security. The ongoing oversight provided by these audits/reviews ensures that DFAT can identify areas for continuous improvement and respond quickly to new and emerging risks.

The Government's revised Protective Security Policy Framework (PSPF), which came into force on 1 October 2018, requires all Australian Government entities to assess annually the maturity of their security practices through a report to:

- their portfolio minister and the Attorney-General's Department on:
  - whether the entity achieved security outcomes through effectively implementing and managing requirements under the PSPF
  - the maturity of the entity's security capability
  - key risks to the entity's people, information and assets, and
  - details of measures taken to mitigate or otherwise manage identified security risks; and to
- other entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in PSPF implementation.

Recommendation No. 4
That DFAT reviews policies and procedures, and implements revised arrangements to ensure consequences for non-compliance are adequate to embed a strong security compliance culture

In developing the DSF, DFAT reviewed its policies and procedures regarding consequences for non-compliance. Our new security breach policy and security clearance compliance framework represent important tools for embedding a strong security compliance culture, together with messaging from senior leadership, training and ongoing communications/awareness raising.

Changes to DFAT's security clearance vetting process now provide stricter guidelines for clearance subjects regarding their responsibility to comply with the clearance process and for the completion and submission of information. There is an escalation process when non-compliance occurs. These changes align with the revised PSPF.

Recommendation No. 5
That DFAT report back to the Committee on the status of its cyber resilience and compliance with the 'Essential Eight' as at July 2018

DFAT had achieved full compliance with six of the 'Essential Eight' cyber security risk mitigation strategies (including the four mandatory strategies) by June 2018. DFAT has made significant progress in implementing the two remaining strategies and is largely compliant, with only minor residual work remaining.

Recommendation No. 6

That DFAT provide a detailed outline of:

(i) how recent improvements to DFAT's systems are providing assurance that staff have received the required security training for their posting

(ii) any further improvements to these systems that DFAT is planning to implement, including timeframes

DFAT's learning management system has been upgraded. Further enhancements are being explored to provide better assurance that staff have received the required security training for their posting.

In addition, and prior to deployment, DFAT staff are required to complete a mandatory training checklist which supervisors are required to sign off before an officer can depart on their posting.

To ensure the effectiveness of DFAT's security training, a Training Needs Analysis (TNA) is being undertaken by external consultants to inform the Security Branches as to the specific requirements for all officers travelling abroad for long-term posting or short-term missions. This analysis will help ensure learning outcomes can be measured and directly linked to staff capability requirements.

Recommendation No. 7

That DFAT:

(i) review the level of support it provides to Canberra-based and out-posted staff regarding post security, with particular attention to the effectiveness of the security training program

(ii) report back to the Committee on the methodology and results of this review

(iii) implement improvements to strengthen the security training program as necessary

The Security Branches undertook an internal review of training in early 2018 in the context of the launch of the DSF. This led to updates to all eight of DFAT's security courses. In particular, one course was adjusted to include additional experiential-based learning through an off-site mock 'health check' and dedicated training sessions on security risk management.

A number of internal training sessions were conducted throughout 2018 for members of the Security Branches to ensure consistency regarding the application of the DSF's risk management tools.

In August 2018, DFAT commissioned an independent review of its security-training program by an external consultant to assess the appropriateness, effectiveness and currency of security training in the department. As a result, a new TNA was commenced in January 2019 to resolve identified gaps in the current training program. The TNA is due for completion by May 2019.

Recommendation No. 8
That DFAT:

(i) mandate the completion of cyber security training for locally engaged staff

(ii) make available to the Committee a summary of key initiatives under the department's security communications program, and outline for the Committee how this program contributes to staff education on cyber security

The 'Cyber Security Fundamentals eLearning' course is mandatory for all DFAT employees (including APS, contractors and locally engaged staff) upon commencement with the Department.

Over the past two years, DFAT has developed a strategic communications campaign program, which is helping to build a robust security culture in the department. Two campaigns in that period have addressed cyber security. DFAT's communication materials have now been shared with and utilised across the public service and by our 'Five Eyes' intelligence partners. The effectiveness and impact of these campaigns are measured through surveys, page views of the Security Branches intranet site, rates of reporting and breach data.

DFAT's 'Security Week' (18-22 March 2018) was a major initiative that contributed significantly to developing a positive security culture in the Department. Activities included an interactive display of security technologies and an experiential learning module. Cyber security was also incorporated into Security Week through a series of presentations on how to protect family and children online.

Frances Adamson
Secretary
Department of Foreign Affairs and Trade

7/03/19