Appendix 1

Questions for Scottish public sector organisations on the draft public sector action plan and draft best practice guidelines on cyber resilience

Please provide comments on the draft action plan and the draft best practice guidelines on cyber resilience in line with the following questions.

Question 1: To provide important context, please give an overview of your current arrangements for cyber security. In particular, please provide details of:

- any relevant accreditations held, or standards met, by your organisation
- current board level, governance and risk management arrangements for managing the cyber threat in your organisation
- any ongoing programmes of work on cyber security in your organisation
- the current level of resource you devote to cyber security in your organisation.

Answer to Question 1

SEStran do not currently hold any accreditations or recognised standards, however, we do have in place a robust arrangement for cyber security, managed through our IT provider. This includes ongoing discussions with our IT provider One Stop IT.

SEStran have a broad range of policies in place, which obtained Board approval before being implemented and are subsequently subject to regular review by key Officers and our Performance & Audit Committee. The policies are:

- Information Security Policy (includes user agreement form)
- Business Continuity Management Plan
- Data Protection Policy
- Records Management Plan (Agreed by Keeper of Records, National Records Scotland)
- Portable Devices User Agreement Form
- Homeworking Policy
- Public Interest (Whistleblowing) Policy
- Disciplinary Procedures
- Terms and Conditions of Employment Contract

SEStran undergo annual audit and scrutiny by our Internal and External Auditors and part of this exercise involves completing corporate governance framework questionnaires, before a compliance statement is issued, which is required for our annual accounts procedures.

SEStran have been pro-active in its approach to Records Management and have implemented a range of supporting policies, to supplement its agreed Records Management Plan.

SEStran provide Induction to all new employees which includes a session on the above policies. We are currently sourcing, along with our IT provider, cyber resilience training for all staff, which will be provided on an on-going basis. We are arranging to carry out tests of the Business Continuity Management Plan and IT systems with our IT provider before the end of the financial year. Finger print recognition will be used for access to laptops and remote device wiping technology will be applied to mobile devices.

SEStran scoped work with the Scottish Business Resilience Centre but cost was prohibitive this financial year.

SEStran are a small organisation, with 10 employees, handling limited amounts of personal data and the level of resource devoted to cyber resilience is proportionate to the risks faced. We hold regular monitoring meetings with our IT provider in order to review arrangements.

Question 2: Please give your views on the draft public sector action plan and best practice guidelines. We would particularly welcome views on:

- Whether there are any key omissions from the plan
- Whether there is likely to be any unnecessary duplication as a result of the plan
- Whether you believe the plan, if implemented, would make a significant difference to levels of cyber resilience among Scotland's public bodies.

Answer to Question 2

The plan is very detailed and robust and there does not appear to be any omissions. From SEStran's perspective, there would not be duplication as a result of the plan being implemented.

The plan would provide a very useful framework and set of standards for organisations to use in assessing their current arrangements and preparing a programme of implementation and subsequent monitoring of cyber resilience measures.

By applying a set of standards across the public sector there should be opportunities for best practice and knowledge to be shared, which will benefit many organisations with limited resources and, in the longer term, should make a difference to the levels of cyber resilience among public bodies. However, the plan is only one piece of the overall requirement to minimise cyber threats and it should be acknowledged that there could be a major cost implication for many organisations to implement the key actions set out in the guidance.

Question 3: Please identify any key implementation challenges for your organisation in respect of the draft public sector action plan and best practice guidelines.

Answer to Question 3

The key implementation challenges facing SEStran are the close proximity of the target date and lack of resources. For the current financial year, budgets have already been committed and being a small organisation, with limited resources, we could potentially be in a situation where we are unable to deliver our published objectives set out in our business plan for 2016/17 and those that we are statutorily required to provide. This could result in causing reputational damage to the organisation.

Whilst recognising the need to ensure strong cyber resilience, without adequate resources in place, the timescales for implementation seem ambitious. A key issue is whether a sufficient programme of planning could be achieved and if proper consideration would be given to the impact of implementation on the organisation and its resources.

Question 4: If you are a public sector organisation that is not subject to the Scottish Public Finance Manual, please indicate whether you would be in favour of adopting the recommendations set out in the draft action plan and best practice guidelines to ensure alignment with other public sector organisations.

Answer to Question 4

With adequate resource and support provided, SEStran would, in principle, be in favour of adopting the baseline recommendations, which we believe are proportionate to the size of our organisation. Measures above this level, we believe, would be disproportionate to the risks faced and size of our organisation.

Question 5: Please indicate whether you would be willing in principle for your organisation to become a public sector cyber catalyst, in line with the description set out in the draft action plan at Key Actions 6 and 7. (Please note: due to practical considerations, not all organisations volunteering are likely to be selected as cyber catalyst organisations)

Answer to Question 5

Due to limited resource, SEStran would not be willing to become a public sector cyber catalyst.