Cyber Resilience: Draft Public Sector Action Plan and Best Practice Guidelines – Request for Comment

1. BACKGROUND

1.1 On 1st August 2017, the Deputy First Minister, John Swinney MSP, wrote to the Chief Executives of all Scottish public service bodies, in his capacity as the Scottish Minister responsible for strategic security and resilience capability, seeking comments on the Scottish Government's Draft Public Sector Action Plan and Best Practice Guidelines on cyber resilience.

1.2 The global cyber-attack on 12th May 2017 which affected more than 150 countries worldwide and had a high profile impact on some NHS services in Scotland, underlined the potential seriousness of the cyber threat.

1.3 The new General Data Protection Regulation, will introduce significant new fines for personal data breaches from May 2018 which reinforces the key role that cyber security has in underpinning digital public services that handle personal data.

2. DRAFT PUBLIC SECTOR ACTION PLAN

2.1 The draft action plan has been produced by the National Cyber Resilience Leaders' Board and its cross-public sector sub-group (CROPS) in partnership with the Scottish Government. It sets out the proposed key actions that the Scottish Government and its partners will take during 2017-18 to help ensure a common approach to achieving higher standards of cyber resilience amongst Scotland's public sector organisations.

2.2 In summary, the draft action plan proposes that Scottish public sector organisations implement, as a minimum, a number of common baseline cyber security standards, as well as adhering to best practice guidelines on a risk-based and proportionate basis by March 2018.

2.3 The Scottish Government has made clear that the public sector must lead by example on cyber resilience and it should not be seen as being optional but viewed as fundamental to delivering organisational objectives. It is expected that all Scottish public bodies will work towards implementing the action plan and best practice guidelines, as soon as possible.

2.4 The Scottish Government will consider how it will support organisations and has indicated that it may make provision for providing practical support, in the form of e-learning packages and walk-through exercises. It will consider whether additional support should be made available to smaller public bodies. This will be determined on the basis of responses to the action plan.

2.5 Scottish public bodies subject to the Scottish Public Finance Manual (which will be updated in line with the action plan) will be required to implement the measures on a risk based, proportionate basis, in order to comply with their duties under the manual.

2.6 SEStran is one of a number of organisations who are not subject to the Scottish Public Finance Manual. However, the Scottish Government has indicated that it will work closely with such bodies to establish a common approach to implementation, again on a risk based, proportionate basis.

3. KEY ACTIONS 2017-18

3.1 The objectives of the action plan are to ensure that baseline levels of cyber security in Scottish public bodies and their supply chains are met and the key actions are:

Key action 1: The Scottish Government will work with Scottish public bodies to ensure they (i) have in place, as a minimum, baseline levels of cyber security within their organisations, and (ii) achieve appropriate accreditation to provide assurance that these standards are being met by end March 2018.

Key action 2: The Scottish Government will work with Scottish public bodies to ensure they are aware of, and can make appropriate use of, services available under the National Cyber Security Centre's Active Cyber Defence (ACD) Programme.

Key action 3: To promote greater awareness of cyber threat intelligence across the Scottish public sector, the Scottish Government will work with Scottish public bodies who are responsible for managing their own networks to ensure they become active participants in the Cyber Security Information Sharing Partnership (CiSP) by the end of March 2018.

Key action 4: The Scottish Government will work with Scottish public bodies to ensure they minimise the supply chain risks to their own cyber security. This will be achieved by developing a proportionate, risk-based policy in respect of supply chain cyber security, including requirements for suppliers under some contracts to achieve appropriate accreditation, which will then be applied in all relevant procurement processes. These requirements will be set out in a Scottish Procurement Policy Note (SPPN) to be published by end 2017.

Public bodies to whom Scottish Procurement Policy Notes does not apply directly will be encouraged to adopt policies in line with these requirements.

Key action 5: The Scottish Government will work with Scottish public bodies to ensure they provide assurance they are meeting their responsibilities in respect of staff training, awareness-raising and disciplinary processes with regard to cyber resilience. Public bodies will be signposted to existing learning resources, and consideration will be given to the provision of additional practical resources.

Key action 6: Informed by the advice of the National Cyber Resilience Leaders' Board, the Scottish Government will publish best practice guidelines for Scottish public bodies that make clear the practice they should be adhering to, on a risk-based and proportionate basis, in order to achieve appropriate standards of cyber resilience. These guidelines will be finalised by end October 2017.

Key action 7: The Scottish Government will introduce a Public Sector Cyber Catalyst scheme, under which Chief Executives of key Scottish public bodies will be invited to agree that their organisations will take forward work to implement best practice in respect of cyber resilience. The Scottish Government will itself become a Public Sector Cyber Catalyst. Appropriate support will be made available to the public sector cyber catalyst programme to help drive this work forward.

Key action 8: The Scottish Government and the Public Sector Cyber Catalysts will commit to sharing learning and knowledge in order to help drive best practice in respect of cyber resilience across the Scottish public sector.

Key action 9: Informed by the advice of the National Cyber Resilience Leaders' Board, the Scottish Government will put in place a monitoring and evaluation framework to help assess progress towards baseline standards and best practice in cyber resilience across the Scottish public sector.

4. DRAFT RESPONSE

4.1 Due to the pressing nature of the cyber threat, Scottish Government have asked for comments within a tighter timeframe than usual and the deadline for responses is 15th September 2017.

4.2 SEStran will draft a response see Appenidx 1 as summarised below:

- Provide details of our current cyber security arrangements.
- Outline key policies in place and the governance mechanism for implementation and review.
- Highlight the size of our organisation and state that resource devoted to cyber resilience is proportionate to the risks we face.
- Comment that the draft documents are robust and provide a useful framework for implementing key actions.
- Ask SG to recognise that there will be cost implications incurred by organisations adopting the plan.
- Identify the key implementation challenges facing SEStran; namely ambitious timescales and lack of resource.
- Acknowledge the need for strong cyber resilience within the public sector.
- State that if adequate resource and support is provided, we would, in principle, be in favour of adopting the baseline recommendations, which are proportionate to the size of SEStran and the risks faced.
- Comment that we would not be willing to become a public sector cyber catalyst due to limited resource.

5. RECOMMENDATIONS

It is recommended that the Committee notes:

5.1 the contents of this report, and;

5.2 that the Chair of the Board will write to the Deputy First Minister outlining SEStran's commitment to cyber resilience but seeking to understand his offer of further funding for small public bodies to undertake the actions within the proposed timescale;

5.3 that a further report will be brought to a future meeting of the Committee when Scottish Government formalise and publish their Action Plan and Best Practice Guidance.

Angela Chambers
Business Manager
September 2017

Policy Implications	As outlined in report.
Financial Implications	Potential impact on budget if no resource provided by SG
Race Equalities Implications	N/A
Gender Equalities Implications	N/A
Disability Equalities Implications	N/A
Climate Change Implications	N/A