Annex B
Cyber Resilience Strategy

RESPONDENT INFORMATION FORM

Please Note this form **must** be returned with your response to ensure that we handle your response appropriately

1. Name/Organisation

Organisation Name

Angus Council

Title **Mr** ☒ **Ms** ☐ **Mrs** ☐ **Miss** ☐ **Dr** ☐ ***Please tick as appropriate***

Surname

Armstrong

Forename

Mark

2. Postal Address

Angus House		
Orchardbank Business Park		
Forfar		
Postcode DD8 1AN	**Phone** 01307 476469	**Email** armstrongm@angus.gov.uk

3. Permissions - I am responding as…

Individual ☐ / **Group/Organisation** ☒

Please tick as appropriate

(a) Do you agree to your response being made available to the public (in Scottish Government library and/or on the Scottish Government web site)?

Please tick as appropriate ☐ **Yes** ☐ **No**

(b) Where confidentiality is not requested, we will make your responses available to the public on the following basis

Please tick ONE of the following boxes

Yes, make my response, name and address all available ☐

or

Yes, make my response available, but not my name and address ☐

or

Yes, make my response and name available, but not my address ☐

(c) The name and address of your organisation ***will be*** made available to the public (in the Scottish Government library and/or on the Scottish Government web site).

Are you content for your ***response*** to be made available?

Please tick as appropriate ☒ **Yes** ☐ **No**

(d) We will share your response internally with other Scottish Government policy teams who may be addressing the issues you discuss. They may wish to contact you again in the future, but we require your permission to do so. Are you content for Scottish Government to contact you again in relation to this consultation exercise?

Please tick as appropriate ☒ **Yes** ☐ **No**

CONSULTATION QUESTIONS

National leadership; Shared responsibilities; Working together; Protecting Scotland's values

Q1 Are the guiding principles right for this strategy?

No ✓

Are there any other principles that should be considered when continuing to develop the strategy?

Generally agree with the guiding principles. However would suggest that ensuring the safety and welfare of citizen, particularly the most vulnerable in society should also be a guiding principle.

The meaning of the phrase "delivery of better outcomes" on page 12, Section 5 under **National Leadership** of the draft strategy is unclear in this context. If it means the aim is to make Scotland and the citizens of Scotland more secure from cyber attack then it would be better to be explicit rather than use the jargon "better outcomes". If it just a general expression of intent to "make things better" then the sentence would be best deleted.

The strategy should provide greater clarity on the practical delivery of 'collaborative leadership'. National leadership is required but so is local leadership particularly if, as the draft strategy details, implementation will be the responsibility of the Scottish Government's partners. Greater clarity is needed on the expectations of local authorities, and other partners, in delivering the strategic outcomes and how these will be resourced.

There is a possible tension between a public body's requirement to ensure its cyber resilience, e.g. the security and protection of its systems and data about its citizens, with the expectation to work more effectively in partnership and across organisational boundaries. Increased collaboration and sharing of data may reduce the overall security of that data.

There should be clear alignment to the resilience strategy and the "Secure and Resilient" strategic framework for Scotland – Critical National Infrastructure; they are inherently linked. Similarly, connections should also be made with the National Action Plan to tackle Child Sexual Exploitation.

Protecting Scotland's Values. We suggest there needs to be clarity as to what these are and reference made to the Human Rights Act, the UN Declaration on Human Rights and the UN Convention on the Rights of the Child.

The strategy would also be improved if it explicitly recognised the fact that scammers and cyber criminals tend to target our more vulnerable citizens. A section that is entitled “Protecting Scotland’s more vulnerable citizens” with a sentence like “our strategy will pay especial attention to the needs and risks to our more vulnerable citizens and link closely with Adult Protection Committees and Trading Standards Departments and teams across Scotland” would be a helpful addition.

Our vision is for a cyber resilient Scotland that is safe, secure and prosperous

Q2 Do you agree with the vision?

Yes ✓ No

Strategic Outcomes:
1. Our citizens are informed, empowered, safe and confident in using online technologies
2. Our businesses are resilient and can trade and prosper securely online
3. We all have confidence in the resilience of our digital public services

Q3 Do you agree with the strategic outcomes?

No ✓

Are there additional outcomes that should be considered?

Strategic outcome 1 – is achievable.

Strategic outcome 2 –not sure how Scottish Government will measure all businesses to be resilient – given many are SMEs and don’t have resources to invest etc.

Strategic Outcome 3 – is having confidence measurable; is it rather that the outcome should be to enhance the resilience of digital public services. Alternatively we recommend adding the word “justifiable” in outcome 3 - confidence in the resilience is not in itself a great outcome if it proves to be misplaced.

We suggest an additional objective could be:
“Attention will always be paid to the needs of more vulnerable people especially people affected by serious health or disability problems”

Key Objectives:

1. *Provide effective leadership and promote collaboration*
2. *Raise awareness and ensure effective communication*
3. *Develop education and skills in cyber resilience*
4. *Strengthen research and innovation*

Q4 Do you think these are the right objectives to focus on?

Yes ✓

Are there additional key objectives that should be considered?

It should clearly state that they refer to the Public, Private and Third sectors.

There could be more emphasis on education, and awareness, particularly for those groups such as older people who may find this more challenging. The strategy could helpfully give specific coverage to those groups who are currently excluded from the digital world (3 in 10) or who may be more vulnerable to cyber attacks through lack of knowledge and confidence.

Objective 1: Provide effective leadership and promote collaboration

Main areas of focus:

- *The Scottish Government to set up and lead a national strategic implementation group to implement, monitor and evaluate the impact of this strategy*
- *The Scottish Government to be at the forefront of providing safe and secure services, and sharing their knowledge with other organisations*
- *Collaborating with partners, the Scottish Government will lead and coordinate efforts to develop national cyber resilience*
- *Ministers and their officials continue to raise the profile of the importance of cyber resilience across a range of policy areas*
- *Ministers report on the Government's progress in building a culture of cyber resilience and good practice across the Scottish Government and its agencies*
- *The standards of cyber resilience adopted by the Scottish Government's on-line services – and those of other public agencies - will be available to service users.*

Q5 Do you agree with the main areas of focus for effective leadership and collaboration?

Yes ✓

Are there other areas that should be considered?

The text on page 15 states that legislation or regulation is not proposed. There should be a statement as to why this is not needed.

Greater clarity is needed on the expectations of local authorities, and other partners, in delivering the objective and how this will be resourced.

Perhaps the same approach to resilience should be adopted in terms of governance and reporting. This has still to be finalised via the resilience strategy; but it would make sense to integrate this work into the existing structures that work and set up a cyber-group aligned to the wider resilience agenda within Scotland

---

Objective 2: Raise awareness and ensure effective communication

Main areas of focus:

- *The Scottish Government alongside its partners to co-ordinate general awareness raising activity to promote a culture of cyber resilience among all Scottish citizens, including promoting the national online safety websites Get Safe Online and E-crime Scotland across Scotland*
- *Stakeholders and partners to implement audience-specific awareness raising activity - targeted at employees, educators, leaders and board members*
- *Working alongside the UK Government, the Scottish Government and partners from across the business world to form a network to share information about online threats and vulnerabilities*
- *Industry professionals develop and promote best practice in cyber resilience*

Q6 Do you agree with the main areas of focus for raising awareness and ensure effective communication?

Yes ✓

Are there other areas that should be considered?

The needs of citizens who have no access to or knowledge of I.T. should be taken into account. In many areas of life from organising money to getting good deals on essentials like fuel, more vulnerable citizens are disadvantaged financially if they do not use IT.

We wonder if there should be a wider campaign to promote this, e.g. similar to community resilience and ready winter, especially for members of the public who perhaps don't always access the same online forums or websites.

In addition, using forums such business breakfasts and through local economic development forums and chamber of commerce audiences. We also think having experienced live examples of how easy it is to hack into a range of devices/laptops etc. if they are not properly protected has more impact that just literature. Showing how many cyber-attacks happen on a single day globally can provide the required shock factor.

Materials should be made available for the audience specific awareness raising activities.

The text on page 18/20 refers to the "…Scottish Government alongside its partners …" Clarity is required as to who these partners are, i.e. private, public and third sectors.

Objective 3: Develop education and skills in cyber resilience
Main areas of focus:

- *The Scottish Government and its partners promote the development and delivery of cyber resilience education in early learning and childcare settings, schools, colleges, universities and other learning settings*
- *Business partners build cyber resilience capabilities within workforces*
- *Scottish Enterprise and other business partners help develop the cyber security and resilience goods and services industry in Scotland*

Q7 Do you agree with the main areas of focus for developing education and skills in cyber resilience?

Yes ✓

Are there other areas that should be considered?

We fully support these objectives but would add "adult education" in the list to ensure it is not missed.

Specify who it is who will develop learning materials etc and how this will be resourced.

The agreement to develop a product for all to use in schools for example would be beneficial with supporting materials. Using the same approach as the Ready Scotland campaign for winter would offer a user friendly and visual solution.

The Scottish Government also needs to build cyber resilience capabilities within workforces.

Objective 4: Strengthen research and innovation
Main areas of focus:

- *The Scottish Government, Police Scotland and partners progress with research to baseline the cost of cybercrime to Scotland*
- *Partners undertake and share research on understanding "what works" in preventing cybercrime, using knowledge from local, national and international angles*
- *Partners work together to target funding for cyber resilience research*

- *Enterprise funding is targeted at innovative methods to support the cyber resilience of individual or groups of enterprises*

Q8 Do you agree with the main areas of focus for strengthening research and innovation?

Yes ✓

Are there other areas that should be considered?

We strongly support this. To keep up with cyber criminals we require a resource designed specifically to do so. However, targeting existing resource at this work would be at the expense of other activity and priorities.

A 5th area of focus could be to actively explore and use learning from other areas.

How will we use the strategy to achieve real change?
For each of the outcomes, the Scottish Government and its partners are developing a detailed action plan setting out the short, medium and long term activities. These specific measures will be published in early 2016. Within this action plan there will be practical activities, projects and improvements to support individuals and organisations to become more cyber resilient, as well as steps to build up the cyber security goods and services sector in Scotland.

Q9 Are there additional actions that will help us achieve making Scotland and its people more cyber resilient? Yes.

This has to be an on-going campaign, otherwise, it will fall off the radar and only those working within the cyber environment will be aware; making sure we are all prepared and aware is the key message.

The sentence under **Implementation** in the strategy might put people unfamiliar with modern "management speak" off. (..high level strategy…overarching driver…)

Plain English throughout this and any further documents to support the Cyber Strategy would make the strategy more inclusive and get the maximum public support.

We suggest inclusion of groups with expertise in taking forward the strategy like the Scottish Business Resilience Centre and The Scotland Group on Financial Harm chaired by Paul Comley, National Adult Protection co-ordinator would enhance progress.

The inclusion of the perspective of individual and business victims of cyber

crime would assist

Links to the National Scam Hub and Trading Standards Scotland would also be useful.

The text refers to “each of the outcomes” – I take it they mean exah of the key objectives.

How will we know if we are succeeding?
The Scottish Government will be asking stakeholders to share their action plans and keep track of milestones and progress on an annual basis. This will help to provide regular annual updates to the national strategic implementation group.

Q10 Do you think the monitoring and evaluation arrangements are sufficient?

Yes ✓

If not, what arrangements would you like to see?

As noted at question 5 – having an advisory board linked to the resilience agenda nationally would be helpful and integrate into the wider resilience and critical national infrastructure work streams. There are other forums which IT representatives use to meet frequently, but this needs to move into a wider audience than IT.

Q11 Have you ever experienced cyber crime (see examples on page 16)?

Yes ✓

If so, did you report it? Please provide details.

Angus Council has a Financial Harm Sub Committee reporting to our local Angus Adult Protection Committee with the specific aim of making Angus citizens as hard to financially abuse as possible. This committee has members from all relevant public bodies as well as the financial services and small business sectors.
We have knowledge of all types of scams including those perpetrated using the internet.

There are also well established joint police/ social work child protection arrangements that are responding to increasing situations where young people are being exploited on line.

Q12 Would you be willing to share your experiences with us?

Yes