St George's House Consultation

# Local Leadership in a Cyber Society

## Towards a model for Civic Cyber Resilience

18th/19th January 2016

In partnership with the National Cyber Security Programme 2015/16 and

Department for Communities and Local Government

iNetwork involve influence inspire

City of London

bcs The Chartered Institute for IT

Windsor Castle College of St George

## Executive Summary

Under the auspices of the National Cyber Security Programme, the Department for Communities and Local Government (DCLG) has been running the *Think Cyber – Think Resilience* programme and developing a model for Civic Cyber Resilience[1], aimed at raising awareness about cyber related risks with senior leaders in local government.

Building on this work DCLG, supported by iNetwork, City of London Corporation and the British Computer Society, convened a group of senior leaders from local government, the wider resilience community and central government to look how the forthcoming 2016/2021 National Cyber Security Strategy (NCSS) and the revised National Cyber Security Programme (NCSP#2) can best reflect the ongoing role of local government and their partners in supporting wider cyber-resilience.

The common challenge faced across the public sector is that from the customer perspective – whether citizens or businesses – the boundary between central and local government is often blurred, ignored or unknown. There is, therefore, a need to take a more holistic, collaborative and coherent approach to public sector cyber resilience. To do so, requires changes for both central government and local authorities. Central government needs to recognise local authorities as partners in delivering cyber resilience rather than seeing them as an end user of their products. Whilst likewise local authorities must collectively recognise the need to prioritise cyber resilience and to better engage with central government where they have the knowledge, expertise and capacity to lead on this agenda.

In common with the St George's House protocol this report looks to capture the emerging consensus of the deliberations; there were points where there was no universal agreement and we have not tried to capture every point or option. However, all the participants were given a chance to comment on a draft report and we have made appropriate changes to reflect their comments.

The consultation discussion commenced with a review of the cyber security landscape at a national and local level, before considering what cyber resilience means from the different perspectives of central government, local government, and that of those working on wider local resilience. The key themes to emerge from the discussions (explored in more detail below) include the:

- Complexity of the cyber eco-system requiring better joining-up and an improved relationship between central and local government.
- Need to raise knowledge and awareness about cyber-resilience including better coordination of cyber-resilience activities.
- Need for mechanisms to help quantify the risks and develop a shared understanding of how resource constraints impact on an organisations ability to deliver new burdens.
- Links between cyber-resilience and culture or behavioural change, requiring an evolutionary approach to the implementation of cyber-resilience strategies.

Having identified the main strategic themes, the consultation then focused on what needs to change so that greater levels of cyber resilience can be realised. The broad strategic recommendations are outlined below with further detail on specific proposed actions and potential pledges of support made against the different aspects of the "Civic Cyber Resilience" model at Annex A.

[1] See draft model and links to key knowledge bank resources at Think Cyber Think Resilience (note the term Civic is used to denote the difference around locality based governance and services as opposed to those of central government, defence and industrial sectors (see http://www.oxforddictionaries.com/definition/english/civic)

- Design a collaborative governance model that reflects the needs and aspirations of both central and local government around cyber resilience.
- Define and publish the role of the National Cyber Security Centre (NCSC) and outline what its relationship will be with local government and how the sector can help inform NCSC development and operations.
- More effective knowledge sharing and awareness so that there are clear channels of communication and messaging between central and local players.
- Build on existing resources, both centrally and locally to leverage prior and new investment effectively.
- Create mechanisms for engaging local government and civic society on the agenda so that they can play an integral part in developing forward cyber security strategy.

DCLG will continue to work with their partners in central government, with local government representative bodies and those who took part in the discussions to determine how best to take forward these recommendations within the wider framework of the emerging National Cyber Security Strategy.

DCLG would like to thank the co-sponsors of the event, Jos Creese (president of the British Computer Society) for facilitating the discussions, St George's House for hosting the event and providing Brian Parry as rapporteur. Also our thanks go to all those who gave up two days from their busy schedules to take part in the discussions and their ongoing support in the production of this report and the continuing dialogue around local cyber resilience.

## Background

Growth in the use of digital technology is increasing at an exponential pace, the 'Internet of Things' is becoming a reality of daily life as more aspects of our lives become digitally connected. As a consequence the number and frequency of disruptive incidents is growing as society becomes more susceptible to cyber threats. Technology continues to evolve at an ever rapid pace and access to the knowhow and technology to launch these disruptive events becomes more easily accessible, there is an 'evident and urgent necessity' to consider how society develops a more robust approach to cyber resilience.

The focus for the consultation was to explore current engagement between central and local government on cyber resilience. In doing so both central and local government would explain how they and their partners are approaching the need for greater cyber resilience so as to become better engaged in the cyber resilience agenda. It was recognised that there are different approaches to cyber resilience by central government and local government. Traditionally the centre has focused on a national perspective in seeking to address issues like security, critical national infrastructure and regulation. Whilst the local government and wider civic sector organisations (covering areas like police, fire, health and local community groups) are increasingly being called upon to focus on cyber incidents impacting on localities and the complex interactions between multiple civic organisations in a specific place/locality. In response to these challenges the consultation participants focused on the following areas of investigation and how they could help to contribute in scoping out a model for local "civic" cyber resilience:

- Provide input from local government and their delivery partners into the NCSS currently being reviewed by central government.
- Consider the role that local government and their delivery partners should play in creating a more cyber resilient civil society.
- Identify practical actions and next steps to support the development of greater cyber resilience in localities.

A key part of the opening discussion was the opportunity to explore and consider the draft "Civic Cyber Resilience" model[2] which DCLG has been mapping with local government and local resilience partners around the building blocks that can help establish a strong cyber-aware culture across local authorities and their partners. Participants where then tasked to focus on and refine a series of "asks and offers" that central government, local government and civic society could make in terms of addressing specific needs to be addressed or to bring practical help to the wider cyber resilience agenda.

A series of breakout sessions then followed that were interspersed with further input from the Oxford Global Cyber Security Centre on the Capacity Maturity Model[3] that has been developed to help measure the degree of maturity a country has in terms of cyber resilience, and practice insights from the Corsham Institute as to what the emerging challenges of working in a cyber society mean on a day to day basis. The consultation concluded with a series of recommendations and practical actions for central government and local government and their strategic delivery partners.

St George's House is grateful to Jos Creese (British Computer Society) for facilitating our discussions, as well as DCLG, iNetwork, City of London Corporation, and British Computer Society for sponsoring

[2] See Annex A Civic Cyber Resilience Model and at Think Cyber Think Resilience
[3] See Oxford Global Cyber Security Centre Capacity Maturity Model

this event. We would also thank the individual speakers who shared personal insights during the consultation on how their organisations are approaching the issue of cyber resilience: such insights and ideas have helped to generate new thinking on how we can collaborate more closely and move towards creating a more cyber resilient society.

This report is structured to highlight the main themes emerging from our discussions as well as the key conclusions and recommendations from the consultation. As with all St George's House reports, this document aims to reflect from an independent perspective the main ideas, themes and views put forward during the event, with the understanding that not everybody involved in the discussions will have endorsed all of the ideas which are represented here.

## The emerging National Cyber Security Strategy

The government is currently updating the NCSS for the period 2016-2021. The National Security Strategy identifies cyber as a Category One threat. The challenge is clear: technology is constantly evolving; the mechanisms and tools to launch a cyber-attack are more accessible, more easily available for sale, and require less IT knowhow and skills to be used effectively.

There have recently been a number of high profile disruptive cyber incidents affecting commercial businesses. However, what is less reported and to some extent under the radar are attacks on the public sector. Whilst the media focus is on significant incidents (covering well know financial sector and communications businesses) the threat to central and local government has received less media attention. However, incidents such as confidential emails being released, or a local authority held to ransom to regain access to its data, have taken place in the recent past. The threat facing all public services including local government and their delivery partners is ever present and growing.

Mitigating cyber risk will require a 'collective effort', across society and therefore, the need to join up to provide a holistic approach. Central government has a special role to play in this process, as there are certain things which only central government can and should do. However, there is a need to recognize the difference between central government with its national focus and local government with its focus on the provision of key services within more narrowly defined areas. The challenge is how to engage local government and their delivery partners in this process.

The NCSS is still in development. In terms of the Government's roles and responsibilities, the Strategy is likely to address the following activities:

1. Establishment of a National Cyber Security Centre (NCSC)[4] to simplify and consolidate the Government's architecture on cyber and provide a single point of contact and expertise to coordinate activities for government and the wider public and private sectors . The full remit of the NCSC is still being worked through but it is likely to build on existing assets and initiatives including CERT-UK, CiSP, CPNI, etc.

2. Build on the UK's world class technical expertise to strengthen our defences and our ability to disrupt the activities of our adversaries, including cyber criminals.

3. Provide a focus on skills development identifying channels to increase our talent pool and address the current gap in terms of demand for cyber skills.

[4] See https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together

4. Grow the cyber security sector thereby facilitating growth of the UK's cyber security industry through innovation, investment and nurturing of new businesses.

The Chancellor has recently announced[5] that £1.9bn of funding will be set aside for the five years through to 2021 to support implementation of this transformative work, although the prioritisation and allocation of this funding has yet to be confirmed by government. However, the four key objectives reflect the focus on wider national requirements rather than place based local cyber resilience.

One of the challenges for the emerging NCSS is the need to reconcile this national focus with the need for more cyber-resilience within localities. The growth of locally delivered public services, and ever increasing interconnections between local and national public service providers, all mean that national cyber-resilience is increasingly dependent on local cyber-resilience. The local delivery landscape is also changing because the devolution agenda is not only restructuring English local government but also creating new freedoms and powers for the devolved administrations. There is, therefore, a need for a more flexible and holistic approach to cyber resilience at the local level, supported by national framework of shared principles, agreed standards, and coordination.

Whilst the new NCSS is to be welcomed, a number of participants felt there are risks of relevancy and unrealistic expectations being set here by these objectives. We need to recognise that NCSS will not be a panacea for all the cyber threats faced by the country, nor will many of the threats addressed by this strategy be relevant to the daily activities of people living and working in the UK. Unless NCSS is positioned correctly as the overarching framework within which a wider programme of co-designed activity sits, there is a potential for a false sense of security being developed by NCSS.

Equally local government and the private sector has not been engaged or consulted to date as part of the NCSS development process. There was a clear request from participants that local government and civic society should be engaged in this process to reduce risks, improve response, give the NCSS greater reach and influence, and reduce costs to the UK overall. Ideally, local government would like to be considered 'partners' in the co-development of NCSS rather than as 'customers' or 'promoters' of NCSS and cyber security.

Further steps towards devolution means that there will be a greater focus on localities for delivery of government services, which may mean greater risks – because changes to existing systems are not cyber-resilient and because cyber-attackers believe there is more value in attacking bigger devolved local authorities than traditional smaller local authorities. It is therefore essential that the NCSS is built on a sound understanding of the issues faced at a local level and that wider civic society is engaged in this process. It was also recognised that the NCSC cannot be expected to engage hundreds of local authorities and the many thousands of organisations that make up the wider civic society in dialogue. Collectively, local government needs to determine how it can effectively engage with the emerging NCSC and how local authorities can be encouraged to take the lead on cyber resilience in their respective localities.

Comparisons were made to the Scottish government's recently published cyber resilience strategy[6]. In Scotland the focus is more about generating resilience within society, rather than defence and deterrence. The Scottish strategy recognises that we will never completely eliminate cyber threats

[5] See https://www.gov.uk/government/news/chancellor-sets-out-vision-to-protect-britain-against-cyber-threat-in-gchq-speech
[6] Safe, secure and prosperous: Cyber resilience strategy for Scotland http://www.gov.scot/Resource/0048/00489206.pdf

rather we can take steps to reduce it and at the same time aims to consider how society should respond in a resilient manner to such threats emerging.

There is also a need to recognise the growing inter-generational changes that are taking place within society, and accept that there is a growing willingness amongst a younger generation to trade data privacy for accessibility to services. Younger people are much more willing to share data online without considering the risks and threats faced. If we are to raise awareness and educate this segment of the population to the cyber threat faced and grow resilience amongst such individuals, we will need to use sophisticated communications based on behavioural theory, rather than simple public awareness campaigns. Otherwise, we run the risk of repeating the authoritarian (and less effective) communications campaigns of the past, which covered social policy issues, such health education (e.g. HIV and 'Don't do drugs').

## The role of local government and their strategic delivery partners

The discussions recognised the different but equally important roles played by national and local government in creating a more cyber resilient society. It was evident that a new approach is required – one based on mutual trust built on national standards but allowing for local flexibility and priorities – if both areas of government are to work together to build a more cyber resilient society.

The devolution agenda will continue to radically change the way that local government and their strategic partners deliver public services. Devolution and increasing reliance on local delivery of public services means that there is a need to consider local government not only as a key 'partner' in the design of the ongoing NCSS but also in terms of its wider implementation plans and programmes.

It is important to recognise that the key differentiator between central and local government is 'place'. Within any given locality, the local authority delivers a large range of services interacting with numerous stakeholders both within the local authority and in other public, private or third sector organisations - all of which adds complexity to managing cyber resilience. Priorities for local government will vary according to the nature of the locality in which they operate. A stark contrast was described between the approach and priorities in a locality like the City of London compared with a more rural locality such as West Suffolk. There needs to be an acceptance that the priority given to cyber security will always vary according to the characteristics of the locality and competing priorities.

However, there is a need for common principles and minimum standards to be set to address an underlying concern that cyber risks are not always featured on local risk registers and need to be better and more widely understood in order to ensure effective management of the growing risk are fully understood by senior officials and leaders within local government. Cyber threats as risks are commonly 'owned' by the IT Director rather than Chief Executive within local government, they are rarely discussed at board level or with elected members, and in many cases there is a lack of knowledge and understanding at a senior level of the risk faced. While there is guidance available on cyber security and resilience, what are needed is more locally targeted/role-based guidance and training for senior leaders, managers, professional heads of services and all local government employees to ensure they understand the potential risks to themselves, their organisations and localities.

Protecting communities is an important aspect of local government's role, alongside that of delivering local services and creating more sustainable and resilient communities. Some argued that

creating more sustainable communities is in fact now the key priority for local government, with fewer resources available we are asking communities to become more sustainable and self-reliant. There is an established network of 38 Local Resilience Forums (LRFs) supporting local communities in coordinating and managing risks. LRFs are complex fora involving multiple stakeholders (e.g. City of London has over 170 stakeholders in its resilience forum) and many of them do feature cyber risks on their local risks registers. There is an urgent need to determine what role (if any) the LRFs will play in developing cyber resilient communities.

Maintaining cyber security and resilience at a locality level requires better coordination between multiple stakeholders. Differing priorities and accountabilities, leads to a patchwork of inefficient competing initiatives and poor collaboration; LRFs may be able to help coordinate all these stakeholders but can only do so under a simplified and holistic approach to cyber resilience based on nationally agreed priorities. Key stakeholders include police or other crime prevention agencies, business representative bodies (including Local Enterprise Partnerships), Third Sector organisations and Health and wider category one and two responders such as utility companies. There is a need to both engage such bodies in local and regional networks but also to explain how they are managed at a national level, especially which aspects of cyber security are handled at each level. For instance, the National Crime Agency has both a National Cyber Crime Unit (NCCU) as well as Regional Organised Crime Units (ROCUs) that have cyber expertise, however it is not clear who should lead on engagement with local government with regards to cyber threats. There is also limited understanding within local government as to who should lead on cyber security communication with local businesses.

The lack of a clear mechanism to quantify the risk of a cyber threat to localities was also identified as an issue for local government. Central government uses the National Risk Register and Critical National Infrastructure mechanisms to identify and prioritise risks. However, it was noted that local government (a key service delivery channel for many government services such as social care, benefits and safeguarding policies) does not feature on the central government risk register! Local government lacks a clear common mechanism to measure the risk and 'costs' of cyber security threats whereas key elements of private sector such as the financial and insurance sectors have a more mature approach to quantifying such risk, and this might offer an opportunity for the public sector to access the skills and knowledge needed to assess and quantify cyber threats.

Local government holds essential local intelligence about communities and cyber risks, which needs to be better managed, controlled and shared as the UK approaches a time when integrated UK intelligence will be essential to protect against cyber threats. A key strength of local government is its experience in joining up services from multiple agencies round the citizen. However, multi-agency working dependent on one local infrastructure is a potential weakness that could be exploited in a cyber-attack. If the NCSS and the NCSP#2 are going to be successful at creating greater local resilience they will need to consider how wider linkages with other public sector partners as well as wider civic society are to be established and maintained going forward.

At the same time we must recognise that the data provided by CESG and CERT-UK suggests that as much as 80-90% of cyber threats could be managed through basic security measures. Following guidelines such as the CESG 10 Steps Guidance[7] can prevent many cyber threats. Whilst awareness of such basic hygiene factors is increasing (from a low base) an emerging issue is who should be responsible for ensuring they are in place. There is clearly an urgent need to clarify what is

[7] Cyber Security for Business: 10 Steps series https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

'expected' of our public institutions and to educate society in general to the threat faced, without creating panic.

Finally, we looked at infrastructure, interconnectivity, basic hygiene and incident reporting procedures. Local authorities provide a large range of services necessitating both complex infrastructures and numerous connections to secure networks (PSN, N3, JANet, etc.). It was suggested that, with the exception of PSN compliance, local government needs to demonstrate a more consistent approach to cyber resilience. Examples given included the uncontrolled proliferation of websites within local authorities, use of social media without clear guidelines and a lack of common cyber security principles.

Local government argues that it does take cyber resilience seriously and has put in place numerous defences but recognises more needs to be done to reduce the need for different secure connections each with their own code of connection requirements. It was also noted that central government needs to be more proactive in raising awareness about guidance, support material and secure infrastructure. For example, recent engagement with local government on the Government funded Cyber Security Information Sharing Partnership (CiSP), the main knowledge sharing platform for cyber security, has seen local authority membership increase from 2% to 50% (and still increasing). Another example is the recent engagement by the National Archives on the role of the Senior Information Risk Owner (SIRO) – a position widely used in government departments but not in local authorities. It is too early to say what the outcome of this engagement will be, but local authorities are now more aware of the SIRO role and National Archives have a better understanding of how this role may work in local government.

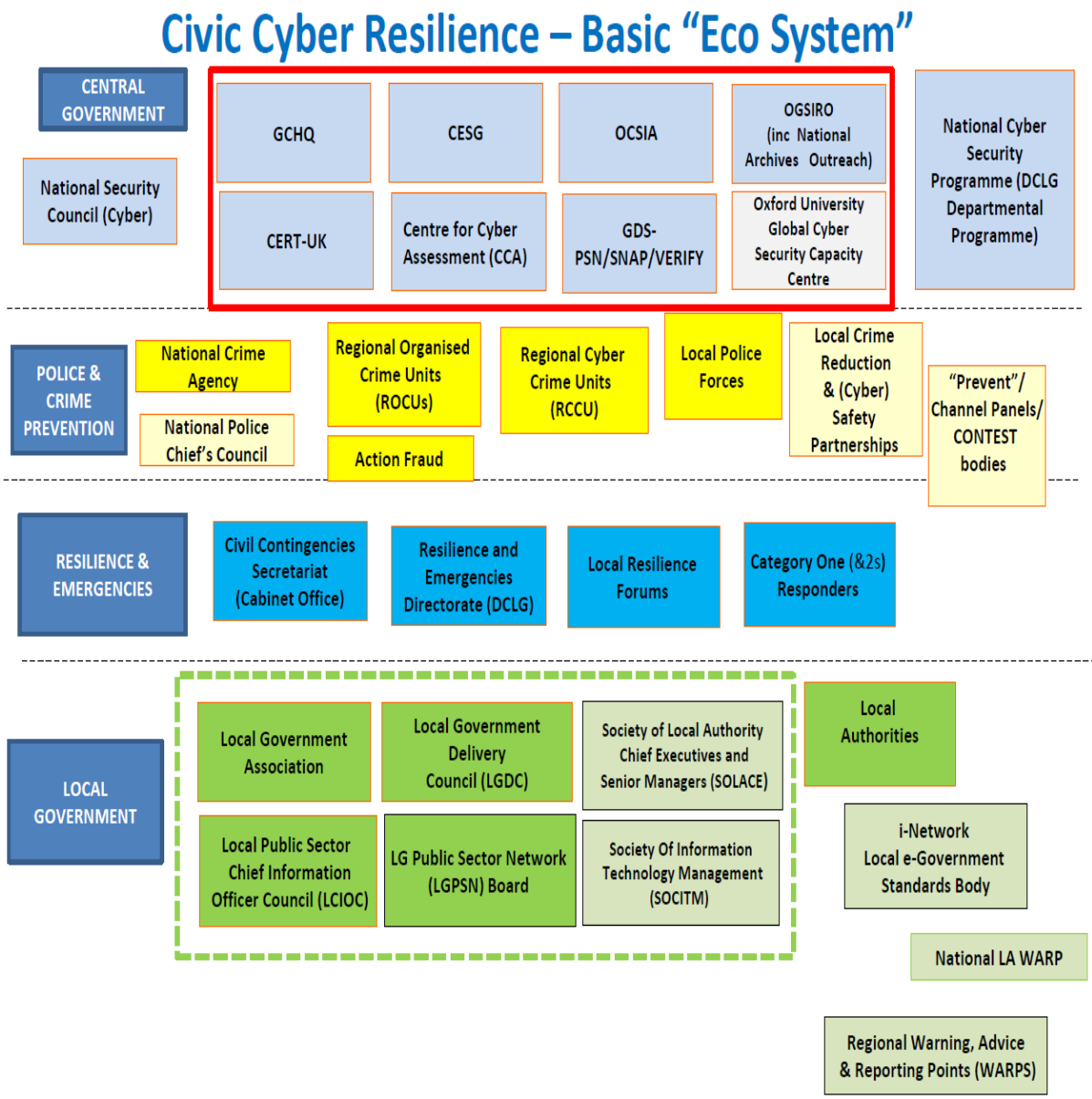
While more needs to be done on these issues, the discussions demonstrated the need for a more collaborative approach around the framing of national guidance, standards and principles around what constitutes good cyber resilience practice and technical implementation as way of better understanding each other's needs and building up mutual confidence in the ability of central and local government to manage cyber security more effectively together.

## Emerging Strategic Themes

A number of overarching strategic issues emerged from this consultation and will need to be addressed if a more cyber resilient civic society is to be created. These are summarised below:

### a) A complex eco-system

The stakeholder landscape for cyber security and resilience is complex, with multiple linkages and no clear hierarchy amongst these different actors and organisations operating within the landscape.




This has created multiple dependencies, overlap and duplication and the conclusion that we are looking at a *"potentially symbiotic"* eco-system rather than a hierarchical model of relationships. Operating within an eco-system generates a number of specific issues that need to be considered:

- Who, if anyone, provides leadership, strategic direction and overall principles/standards?
- The potential for significant duplication of activity and resource inefficiency.
- The functional links between the various groups and organisations.
- Potential for confused and fragmented messaging, with multiple actors all targeting the same recipients of communication with slightly different messages.
- The importance of knowledge sharing if a consistent approach is to be delivered.

It was suggested that a key role for the newly established NCSC should be to help provide direction and co-ordination to this complex, costly and highly fragmented eco-system; however, it was unclear how and when such a decision will be made?

## b) Relationship between central and local government

Within the complex eco-system of relationships discussed above, there is also a clear need for a more collaborative style of working between central and local government – one that can focus on ensuring the cyber resilience of both services and service users whether citizens, business or other parts of the public sector. At present the relationship is characterised by a lack of understanding and trust on either side: central government has traditionally taken directional and compliance based approach to cyber security with local government, who in return have viewed central government as too quick to control or sanction without an understanding of local impact, and offering limited flexibility in terms of how policy should be implemented in differing localities.

With the continuing focus on devolution there is a danger of yet further emphasis being placed on local government and their strategic partners for implementation of government policy and services, without a strong working relationship. The issues of trust, understanding and flexible delivery need to be addressed as matter of urgency – a more mature partnership is needed. The tendency to use league tables (which often seems like a 'name and shame' approach) to highlight weaknesses in local government implementation of policy is seen as particularly unhelpful. Whilst transparency and publishing of league tables can be useful in terms of motivating change, it can lead to weaknesses being made public; it can also reduce at times the degree of trust and collaboration between central and local government. This was seen as not being conducive to a more constructive approach to partnerships that cyber resilience will require.

At the same time, it should be recognised that engaging with local government can be a complex task – there is no single communications channel for central to local government and vice versa. There are often multiple organisations to contact at the local level, as well as representative bodies (such as LGA, SOLACE, and SOCITM) who can be useful channels to specific stakeholders within local government. However this needs to be better understood and mapped, so that dialogue between central and local government can be enhanced. There is also an onus on local government to self-organise so it is able to present a collective and joined-up voice to central government (if only on cyber resilience matters).

In conclusion there is a need to identify a more structured mechanism to encourage greater dialogue between central and local government, and more partnership based approach to working if the NCSS and its implementation are to be taken forward as efficiently as possible.

## c) Knowledge and awareness of cyber security and resilience

There is currently a low level of awareness on cyber security and risks amongst local government leadership at an executive and political level, as well as at an operational level. Anecdotally, it is thought that awareness of cyber risks is mostly within IT departments, more needs to be done to raise cyber awareness with staff and managers in all departments. The PSN network undertakes compliance based audits and can already anecdotally identify those local authorities which have the least knowledge and expertise in terms of cyber security and resilience. It is likely that other secure network providers, who also undertake compliance based audits, will have similar supporting evidence. This variable skills base needs to be addressed if we are to create a more consistent approach across local government and their strategic partners; however, it is unclear who should be responsible for delivering such knowledge transfer?

Awareness is variable, and many local authority leaders struggle to keep abreast of how cyber threats can seriously impact on the workings of their authorities and wider life of the localities they serve. Recognising the growing importance of public service delivery through local government, there is a need to focus on what levels of resilience are already in place, and consider how we can encourage cyber threats to be taken more seriously by local government leaders.

At the same time, central government needs to consider how it can help to educate local government and their strategic partners more effectively to the risk they face. There is a need to move away from a compliance based assurance model to one where there is a growing understanding of the issues and potential impact, as well as an acceptance that taking a more resilient based approach to cyber security is the appropriate way forward for local government. The need for consistent cyber security principles, the definition of minimum standards and a sense of shared ownership of policies, procedures, and practices could well assist local government understanding of their role in the wider cyber resilience agenda and what is expected of them.

### d) Existing knowledge and activities

The recent *Think Cyber Think Resilience*[8] briefing programme has identified that there is already significant activity being undertaken at central and local level in terms of cyber security and resilience. The majority of this activity however is uncoordinated both in terms of delivery and sharing of knowledge and best practice. There are examples of successful local initiatives being undertaken both within local government and also the wider civic society (e.g. like the Gloucestershire local safer cyber forum). However these activities are focused on single geographies, the knowledge and experience is not easily available and therefore the initiatives and expertise remains locally based.

CiSP was recognised as the main government sponsored platform for sharing such knowledge and best practice. However at present there is inconsistent membership and engagement with the platform. Local government has limited understanding of CiSP and demonstrates a limited willingness to share examples of security breaches, issues faced or to request support from others with practical experience of threats being faced using this platform. The need to clarify the potential relationship between CiSP and the local Warning, Advice and Reporting Points (WARPS) was also seen as a key issue going forward.

At the same time the established network of LRFs does not seem to have engaged with the cyber security agenda, and has not demonstrated a willingness to engage with the cyber resilience agenda. A recent initiative designed to encourage each LRF to nominate a cyber contact-point, has led to a handful of responses from the LRF community. This is clear evidence of cyber resilience not being considered an important issue and needs to be addressed.

The lack to date of a single-point-of-contact within government for cyber security and resilience matters was also seen by many as a key weakness in the current eco-system. It is important to recognise that for many public servants (in both central and local government) that cyber security is still a relatively new topic, and that when issues arise there is a need for specialist advice and guidance. However, the lack of engagement with CiSP demonstrates that at present it is unclear what, if any, central resource is available to provide such support and guidance?

[8] See Think Cyber Think Resilience

### e) Quantifying risk

Clear mechanisms exist for quantifying cyber threats and risk within central government and the private sector especially in financial services. However for local government and their strategic partners there is no clear mechanism for identifying and quantifying cyber risk. Care will also need to be taken to ensure that appropriate mechanisms are used by the sector rather than just adopting mechanisms developed by and more suited to other sectors. There is a danger of falling between the national risks registers (identified by central government and crime prevention agencies), and that of the private sector.

It was noted that central government identifies critical national risks and has resilience strategies for what could be described as 'high profile' cyber related risks. However, local government with its focus on the delivery of government services in a specific locality, does not feature on such national risk registers even though the impact on citizens locally could be significant if such services were not available due to a cyber issue.

Local government lacks the relevant tools to both identify and quantify cyber risks, and there is a potential role for the NCSC to help define minimum standards and ways to quantify such risk, as well as to provide expert knowledge and resources to support the development of resilience plans. Without appropriate mechanisms to identify, quantify and record risks; how can local government demonstrate to central government, strategic partners or their service users that they are taking proportionate measures to manage the risks?

### f) Resource constraints

There is a general acceptance within government (both central and local) of the need to implement change in a more resource constrained environment. There is nonetheless a need to ensure the resources allocated for creating stronger cyber resilience are appropriately prioritised and allocated. Local government wishes to have a role in helping to determine priorities, and has experience in terms of making the case for locality based requirements.

Austerity is creating an impetus for new ways of working including integrated shared working and with no-cost or low-cost approaches. These need to be explored further alongside the use of behavioural theory approaches to communications, as part of a joined-up and holistic approach to cyber resilience.

### g) Culture and behaviour change

An underlying theme for many of the strategic issues noted above was the need for successful behavioural and cultural change across the local government sector in order to drive successful outcomes. It was felt that creation of a strong 'cyber-aware' culture across local public services and 'place' will be essential if collaboration and information sharing is to be truly effective. Mitigating cyber risk will require collective effort across society and the public sector – both local and central. It will also require behavioural change in both citizens and public employees in how they interact safely with the cyber world at home and at work.

The plethora of stakeholders within the 'symbiotic' ecosystem will also necessitate creation of a strong collaborative culture around a common goal if strong leadership on local cyber resilience is to be achieved. Such leadership and engagement, based on behavioural change theory, should deliver

the nudges required to ensure that the 80-90% of cyber threats that can be mitigated through basic security measures are indeed countered.

Awareness of cyber security and risks amongst local government leadership at executive and political level, as well as at an operational level, is essential. In resource constrained organisations with lots of competing priorities, like local authorities, the lack of local political awareness is a significant risk to cyber-resilience being seen as a significant priority. There is a need to make the business case for cyber-resilience, including the use of strong communications and engagement activity to create a 'cyber-safe' culture and drive behaviour change at all levels that places public trust, public service and public protection at the heart of public service delivery and policy making across localities.

### h) An evolutionary approach to implementation

Finally, there was general consensus of the need for change to commence as soon as possible, and there is a need to take an agile approach to implementation of the NCSS; one that expects and allows for adjustments as our collective understanding of the local civic cyber-resilience landscape evolves and more mature approach to cyber-risks develops. Such an approach is preferable to a further delay to allow for more planning, and recognises the urgent and immediate need for action.

Central government was therefore urged to consider a phased approach to implementation, starting with smaller short-term joint initiatives with a group of local authorities (as with the Universal Credit programme pilots) looking at what might constitute best practice in terms of cyber related organisational leadership and technological design. This "observatory type" approach would allow for the NCSC to observe and evaluate such initiatives and refine plans as central and local government learn what works and where changes are required.

## Creating Stronger Civic Cyber Resilience: Key Proposals and Recommendations

Having identified the main strategic themes, the consultation focused on what needs to change so that greater levels of cyber resilience can be realised. This next section of the report focuses on the main changes which were identified and who should lead/support each of the recommendations. Please note that only the main strategic recommendations have been outlined here, with further detail on specific proposed actions and pledges made against the different aspects of the "Civic Cyber Resilience" model at Annex A.

### 1. Design a collaborative governance model

There is a need to develop a new governance model for strategic planning and coordination of activities within the eco-system of stakeholders operating in cyber security and resilience. Local government wants central government to acknowledge the wider role of stakeholders as partners not recipients of the strategy. A partnership approach with stakeholders working towards shared objectives would make it easier, faster and simpler to implement cyber-resilience planning, it could also help to avoid expensive duplications of effort and makes better use of resources. Partnership working in turn could help to facilitate the definition of responsibilities in the eco-system, and ensure relevant stakeholders are fully engaged its wider implementation.

Central government needs to recognise that local government and civic society are playing a crucial role in the delivery of government services and a mechanism needs to be found to recognise this critical role as part of the risk assessment process. At the same time, local government must recognise the need for collective agreement on a governance model and the delivery of the cyber-resilience implementation plan. The need for a critical path to deliver the outcomes of NCSS by 2021 was identified as a key component of the new governance model, and this needs to be co-produced rather than being only developed by central government.

The development of this new governance model, that can reflect the needs and aspirations of both central and local government around cyber resilience, should be facilitated by NCSC, but have significant local government input (see later recommendation with regards to the Local Government Cyber Board). The governance model should also be clear how the NCSS will be aligned with the existing serious and organised crime model (4Ps: Pursue, Prevent, Protect, Prepare) which is the basis for much of the cyber security activity to date, and demonstrate how priorities will be set, budget allocated and activities coordinated and measured.

### 2. Define and publish the role of National Cyber Security Centre (NCSC)

Linked to the new governance model is a need to clarify the role and purpose of NCSC, and to confirm the balance between strategic planning and actual delivery.

There is an urgent need for a single-point-of-contact for government (central and local) on cyber security and resilience. However it is unclear if delivery of this requirement will form part of the remit for NCSC.

The recommendation is that NCSC should assume responsibility for both strategy and operational delivery of NCSS as follows:

- Assume responsibility for the development and publication of central policy standards.
- Issue good practice guidance and key performance indicator targets.

- Create a national programme of training and awareness of resources.
- Coordinate the delivery of specialist advice and support to local government to overcome knowledge gaps.
- Provide support during specific emergencies.

The concept of a NCSC relationship manager or cyber advisor for specific local institutions as proposed is one way in which better support and guidance might be offered by the NCSC. The measurement and reporting on progress achieved against key indicators was also identified as a potential role for the NCSC. A priority action in support of this was that early consideration should be made as to how local government can help to play an active role in the NCSC governance and the co-design of solutions, advice and support processes so that it is grounded in an awareness of local community and business priorities and ways of working.

Alongside this is the need to consider options for developing local partnership opportunities between public, private, voluntary and academic sectors to boost localised cyber resilience that can complement proposed NCSC national capabilities and allow the NCSC to target prioritised areas for action in the knowledge that localities have some shared capacity to respond.

### 3. More effective knowledge sharing and awareness

Recognising that there is variable knowledge amongst local leaders, politicians and staff about cyber-resilience; local government needs to consider how communication and knowledge sharing can be strengthened across the local sector. Through CERT-UK and the CiSP platform, central government has the mechanisms to facilitate greater coordination of threat briefings, sharing good practice, and promoting wider discussions.

There is a need to firstly create a common lexicon and to consider communication mechanisms which can raise awareness of the issues in a manageable way with both leaders (executive and political) as well as staff. Good practice guidance needs to be reviewed and made available, and should include guidance on cyber security aspects of commissioning and procurement.

At the same time there is a need to review how knowledge can be shared more effectively and how clear channels of communication and messaging between central and local players can be made more effective. CiSP as a platform needs to be promoted in terms of its role, purpose and use to local government, and all local government organisations should be encouraged (or even mandated) to become members. CiSP should be seen as the main knowledge sharing platform, and usage encouraged through promotion of the benefits and value which it can deliver. This will require a review of the templates and reporting mechanisms to ensure that participants are able to report incidents and share knowledge in a common format.

### 4. Build on existing resources

It will be important for the implementation of the NCSS to build upon the large range of existing initiatives and resources already deployed to support the development of cyber resilience in civic society. There is a pressing need for both central and local government to identify what works and collaborate more closely by pooling funding and skills/talent together so they can maximise the potential leverage from existing resources.

Key to achieving this outcome will be the comprehensive mapping as to what existing resources are already available (in the form of initiatives, tools and communications collateral) to identify how

these can be better coordinated and exploited as part of a low or no-cost approach to extending the reach and effectiveness of knowledge.

DCLG's *Think Cyber – Think Resilience* programme using the draft "Civic Cyber Resilience" model has started to map how these resources can be related to the work of local authorities and their delivery partners. Alongside this, CiSP needs to be used more effectively by local authorities as a knowledge sharing platform (especially for the local sector network defender community) to encourage greater exploitation of the assets which already exist.

At the same time, we need to encourage greater inclusion of cyber issues within the LRF agenda and ensure that wider public sector (e.g. crime prevention, Local Enterprise Partnerships) are engaged and utilised both as communication channels and partners in NCSS delivery.

### 5. Create mechanisms for engaging local government and civic society on cyber security

There is a need to consider how engagement between central and local government can be strengthened to improve dialogue, as well as trust, if the NCSS is to be implemented effectively at a locality level. The intention should be a symbiotic relationship to help resource and develop local capacity to ensure secure operation of joined-up services such as those involving DWP and DVLA.

Participants identified the need for raising awareness amongst local government leadership both executive and political, but more importantly there is need to consider how to encourage behaviour change at all levels to ensure that cyber security and resilience is recognised as an important strategic and operational risk facing any public body. Clear guidance about what risks to consider and recent case studies were seen as important features in terms of creating realistic and useful communication for senior leaders and staff within local government. Embedding cyber into the thinking of senior managers and the development of junior or middle managers requires making awareness of cyber resilience part of their ongoing professional or leadership training.

The Local Government Association (LGA) makes some representations on behalf of its members on cyber security. However this was not considered sufficient particularly in terms of senior level engagement across local government and civic society. A specific local government Cyber Board/Advisory Panel was recommended to support greater dialogue with central government and the team developing the NCSC. Areas identified where local government organisations could help in providing an early focus in formulating next steps were seen as:

- Expand their information governance work to 'mainstream' cybersecurity into local government service areas and initiatives e.g. adults' and children's social care, devolution and smart cities.
- Work with suppliers to ensure that procurement mechanisms (e.g. Digital Services Marketplace and Crown Commissioning Services) embrace relevant cyber security accreditation.
- Collaborate in developing and distributing campaigning and briefing materials for use by local government, police forces and other stakeholders to target different audiences.

However, how the proposed local government (and local partners) Cyber Board would be created and supported was not discussed, although it was suggested that it should have regional representation from across local government so that the views of a wide range of institutions could be collated. The regional nature of Cyber Board representation would also help to raise awareness amongst senior leaders within local government of the risks faced, and also provide central government with a more accessible communications channel to local government on the issue of cyber security and resilience.

Recognising that getting senior leaders to understand and accept the importance of cyber security and resilience, it was also proposed that there should be a cyber-summit for Chief Executives and Chief Information Officers of local authorities (possibly co-hosted by LGA/SOLACE/SOCITM) but sponsored by central government and addressed by Ministers.

## Conclusions

The overall conclusion from this consultation was that society faces an ever present and growing threat in terms of cyber security, and that the UK response to the threat requires much better join-up between central and local government. This includes how we can better organise and manage our resources to both protect society from this threat but also to create a more resilient approach to cyber risks.

There is already a significant amount of activity being undertaken at a local level in terms of cyber security and resilience, however there is also considerable variability across localities in terms of knowledge and understanding of the issues and risks, and a concern that without an overarching strategy to coordinate cyber security activities there is a danger of a fragmented and uncoordinated approach. Moreover, understanding is not mature in general and tackled separately from other emergency planning activities in local government.

We need to recognise that no single body can take full responsibility for delivering cyber security and resilience for society. However, the creation of the NCSC and the development of the new NCSS present a unique opportunity to explore a central/local partnership approach. A stronger, more partnership based approach between central and local government is needed if the design and delivery of the NCSS is to be effective, especially in varied localities and across the wider civic community. This will require the development of new collaborative models that can support better trust, understanding, and joint decision making. The case for this has not been made yet, but this consultation has indicated how such a case can clearly be made to justify a new approach, respecting local and national interests and differences.

There is already much good work being undertaken at a local level but it is fragmented with very limited evidence of sharing of good practices. Local government needs to create stronger messages which will ensure that all local leaders are aware of the cyber security risks faced. That they ensure that their respective organisations and strategic partners have fully considered all such cyber threats. That they have appropriate and tested plans in place to generate resilience at a locality level and ensure quick recovery from an incident, if necessary. Central government can help by building on the current assets like CiSP, providing clearer guidance for local leaders and their partners built around a shared understanding of “Civic” Cyber Resilience all underpinned by a clear set of common policies and standards could help to facilitate this change.

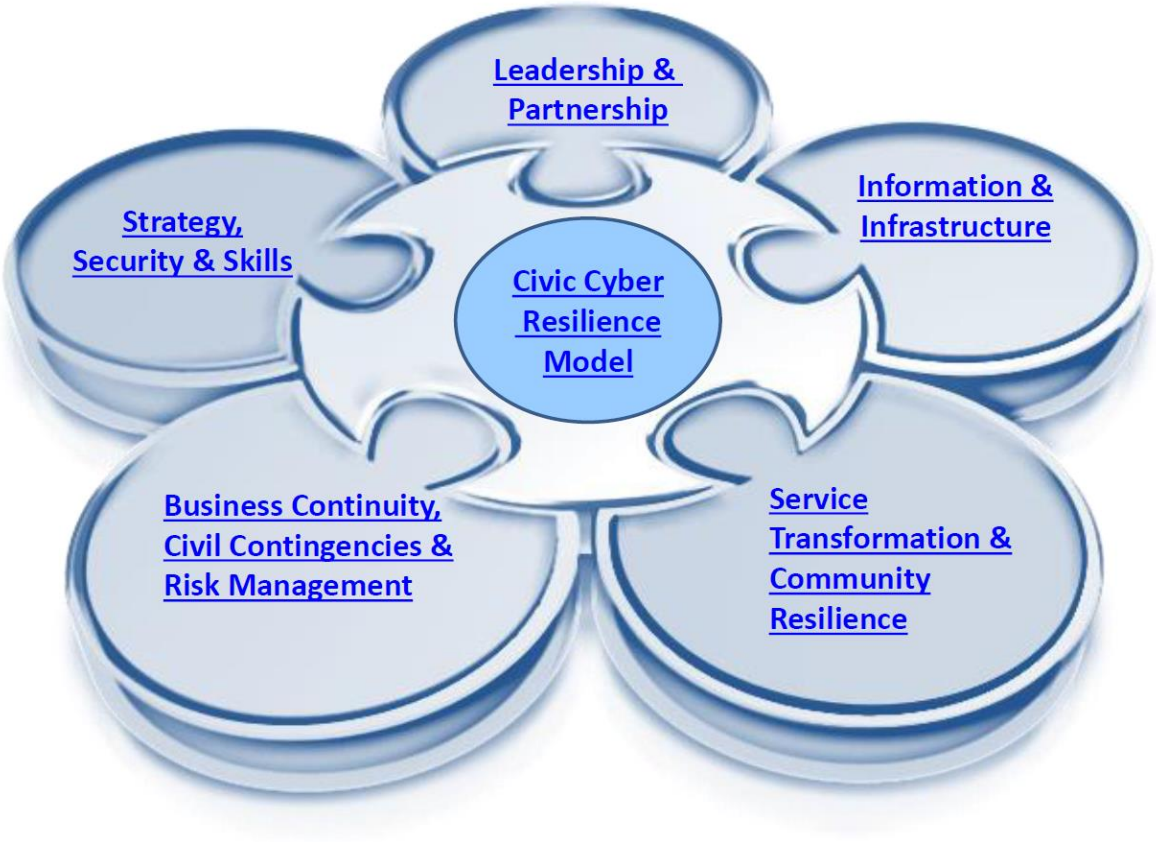
Taking this approach will by 2021 have helped to transform the nature of local cyber resilience so that it places public trust, public service and public protection at the heart of public service delivery and policy making across localities.

Timing is of the essence as we all face growing and evolving threats, with local institutions on which we depend on for delivery of government services, facing daily cyber threats. Implementation needs to start immediately and the network of stakeholders created at this consultation, together with the recommendations to improve communication, sharing of knowledge and coordination between different local agencies can start this process, and hopefully lead to a more robust and resilient approach to the cyber threat faced.

## Annex A: "Civic Cyber Resilience" Suggested Next Steps, Actions and Aspirations to 2021

DCLG working with Local Government and resilience partners has been mapping draft "Civic Cyber Resilience"[9] model built around 5 themes each supported by a series of design principles. The model is intended to support the creation a people focused culture that sees cyber resilience first and foremost as a people issue and proactively creates a strong cyber-aware culture that comes to be seen as everyone's responsibility across civic organisations and their partners.

The draft "Civic Cyber Resilience" model (outlined below) has been tested through DCLG's regional briefing seminars, and inputs from St George's House Consultation participants. The intention being is to make the revised version publically available alongside the forthcoming new NCSS.




This annex sets out a high level view of the consultation participants suggested next steps, actions and medium/long term aspiration to 2021 as built around the model's 5 areas which formed the basis of much of the consultation and working sessions' discussions. These set-out in particular the areas that organisations identified where they could either individually or in partnership with others help to make a contribution to supporting wider cyber resilience across localities and the local public sector.

[9] See draft model and links to key knowledge bank resources at Think Cyber Think Resilience (note the term Civic is used to denote the difference around locality based governance and services as opposed to those of central government, defence and industrial sectors (see http://www.oxforddictionaries.com/definition/english/civic)

| CONSULTATION THEME[10] | SUGGESTED NEXT STEPS AND ACTIONS | MEDIUM/LONGER TERM (2021) ASPIRATIONS |
|---|---|---|
| **STRATEGY, SECURITY & SKILLS - helping to understanding the bigger picture and how stronger cyber security and skills are essential to building and maintaining organisational resilience.** | • Need for local stakeholder dialogue with Government around National Cyber Security Strategy and the "National Cyber Security Centre" proposals (OCSIA, DCLG, CESG and LGA)<br>• Look at extending the *Think Cyber – Think Resilience* programme to cover and senior level briefings /exercises (DCLG)<br>• Look at the scope to co-producing guidance and training (with the view of embedding cyber into wider leadership/ professional development. (LGA, SOLACE,SOCITM and Corsham Institute) | • All LAs fully active on CiSP both at regional and sector level.<br>• All LAs have embedded 10 Cyber Steps across their corporate governance and business processes.<br>• Universal take-up and adherence to Cyber Essentials Plus scheme by default as part of LAs security management and compliance regime(s) to support the adoption of Common Technology Services and Secure Networks<br>• All localities have access to an "NCSC" accredited Local Cyber Resilience professional qualification scheme that underpins the development of a wider local Cyber Resilience profession |
| **LEADERSHIP & PARTNERSHIPS – helping to understanding the role of local leaders and how local resilience forums and their partners should work together to address cyber threats** | • Need to scope out collaborative governance and consider the future role of a possible "Advisory Group on Local Cyber Resilience" (DCLG, LGA,SOLACE and SOCITM)<br>• Put Cyber Resilience on meeting / forum agendas to promote awareness – also self-organise, use existing forums (LGA, SOCITM and SOLACE).<br>• Look to establish a network of Regional Cyber Chief Executive Champions (SOLACE)<br>• Develop a Local Cyber Leadership "Think Piece" publication based on the St George's House discussions (iNetwork, Corsham Institute and DCLG).<br>• Investigate what might constitute "observatory type" approach to testing cyber related organisational leadership and technological design. (DCLG, City of London iNetwork and potentially the NCSC)<br>• Look at clarifying the relationship between CiSP and local WARPSs ( CERT-UK,NLAWARP and SOCITM)<br>• Consider options developing local partnership opportunities between public, private, voluntary and academic sectors to boost localised cyber resilience to complement NCSC national capabilities. (All) | • LAs to own and exercise cyber incident response plans - to support this robust local exercise regimes are in place (local, regional, partnerships, cross-sector, etc.) to test capacity/capability to recover from cyber incidents.<br>• Each LA has a designated Cyber Resilience Champion that form part of a national network linking to the National Cyber Centre. |
| **INFORMATION & INFRASTRUCTURE - having the right Information Assurance/Information Governance and underpinning secure Infrastructures in place to support cyber resilience.** | • Work together on developing a possible online one-stop-shop for localities on Cyber Resilience that will be accessible via CiSP and other related platforms (All)<br>• Look to establish best way forward to create common standards and maturity models for the local sector. (NLAWARP, iNetwork Oxford Martin and SOCITM)<br>• Embed the linkage between Cyber Essentials and secure network compliance (GDS and SOCITM) | • Operational on the Verify platform and other GDS sponsored platforms/registers to secure public trust and operational efficiencies.<br>• Widespread adoption of common technology service blueprints and technical standards<br>• A comprehensive mapping of locality based connectivity touch points to the Critical National Infrastructure has been completed.<br>• A common fame work of basic standards is in place – based around internationally recognised models and approaches. |

[10] Based on the DCLG and local government/resilience partners work on mapping a draft "Civic Cyber Resilience" model built around 5 themes that can help to underpin best practice in local cyber resilience

| CONSULTATION THEME | SUGGESTED NEXT STEPS AND ACTIONS | MEDIUM/LONGER TERM (2021) ASPIRATIONS |
|---|---|---|
| **BUSINESS CONTINUITY, CIVIL CONTINGENCY & RISK MANAGEMENT - being aware of the challenges to business continuity and risk management and how this relates to Local Authorities responsibilities under the Civil Contingencies Act for advice and guidance to local communities and businesses.** | • Work together around developing Cyber Resilience Operating and Capability models that can underpin local authority/local resilience community collaboration. (iNetwork, SOLACE, NCSC and City of London Corporation & City of London Police )<br>• LG and Police colleagues to look at closer partnerships issues, including sharing intelligence within and between sectors (LGA, SOLACE and NCSC)<br>• Template the Local Cyber Safety partnership model for wider adoption (Gloucestershire Police and partners) | • Access to common Business Continuity Planning guidance and advice (building on the City of London model) that can be readily disseminated to help support local enterprises and local service providers.<br>• Operate under a clear definition of the Risk articulated through the National Risk Register and National Risk Planning Assumptions with clear expectations (a robust common methodology) of how LRFs and LAs will be played into the response.<br>• A network of Local Cyber Safety Partnerships (like the Gloucestershire model) is in place to provide peer-to-peer cyber awareness support for Business and Citizen at a local level. |
| **SERVCE TRANSFORMATION & COMMUNITY RESILIENCE - having an appreciation of how good Cyber security can underpin Digital Service Transformation and supporting wider Community Resilience.** | • Consider mentoring support packages for Chief Executives and Councillors – that links cyber to major issues like devolution, heath & social care, digital transformation (LGA and SOLACE)<br>• Roll-out of the Civic/Local Cyber Resilience Draft model and supporting *Think Cyber – Think Resilience* seminar outputs to support Community Resilience (DCLG, iNetwork, NLAWARP and SOCITM)<br>• Support awareness of wider cyber and resilience issues in Central and Local Government through ongoing dialogue and the programme of Thought Leadership work being undertaken at St George's House on Digital Society (Corsham Institute and partners) | • Adopting the official Crown Commercial Service (CCS) Cyber procurement frameworks on Digital Market place and actively promoted via the Commissioning Academy.<br>• Localities have embedded appropriate cyber resilience standards in their Smart city and Resilient Community frameworks. |

## Annex B - Participants

| | | |
|---|---|---|
| Mr Nicholas Alexander | Office of Cyber Security and information Assurance (OCSIA | Cabinet Office |
| Dr Maria Bada | James Martin Fellow | Global Cyber Security Capacity Centre |
| Mr Stephen Baker | Chief Executive | Suffolk Coastal and Waveney District Councils |
| Mr William Barker | Deputy Technology Leader (Strategy, Resilience & Futures) | Department for Communities and Local Government |
| Mr John Barradell | Chief Executive | City of London Corporation |
| Mr Richard Berry | Assistant Chief Constable | Gloucestershire Constabulary |
| Ms Helen Braithwaite | Head of Resilience | Department for Communities and Local Government |
| Mr Mark Brett | Honorary Visiting Fellow (Cyber Security) | De Montfort University |
| Miss Siobhan Coughlan | Programme Manager | Local Government Association |
| Mr Jos Creese | Chief Executive | CCL |
| Mr Ian Dyson | Commissioner | City of London Police |
| Mr Stephen Fear | Community Intelligence Manager | Northumberland County Council |
| Mr Martin Ferguson | Director of Policy & Research | SOCITM |
| Mr Mick Free | Civil Protection Consultant | MF-EP Ltd |
| Ms Noelle Godfrey | Head of Digital Infrastructure & Connecting Cambridgeshire Programme Director | Cambridgeshire County Council |
| Professor Michael Goldsmith | Senior Research Fellow | Global Cyber Security Capacity Centre |

| | | |
|---|---|---|
| Mr Bob Kamall | Programme Manager (Local Cyber Resilience) | Department for Communities & Local Government |
| Mr Peter Lisley | Assistant Town Clerk | City of London Corporation |
| Mr Gary Locker | Contingency planning and business continuity manager | City of London Corporation |
| Ms Chloe MacKenzie | Office of Cyber Security and information Assurance (OCSIA) | Cabinet Office |
| Mr Ian McCormack | Tech Director | CESG |
| Mr Graeme McDonald | Director | Society of Local Authority Chief Executives |
| Mr Tim McSweeney | DCLG Technology Strategy, Resilience and Digital Futures | Department for Communities and Local Government |
| Ms Helen Olsen Bedford | Local Digital Programme | Department for Communities and Local Government |
| Mr Brian Parry | Partner (Rapporteur) | Brian Parry Associates LLP |
| Mr Darren Scates | Technology Leader | Department for Communities and Local Government |
| Mr Mark Smith | PSN Head of Compliance | Cabinet Office - Government Digital Service |
| Mr Phil Swan | Partnership Director | iNetwork |
| Mr Jeffrey Thomas | Director | Corsham Institute |
| Miss Ruth Walker | Resilience Team | City of London Corporation |
| Mr George Woodhams | CERT-UK Engagement Team | Cabinet Office |

## Annex C: Glossary

**CERT-UK** United Kingdom Computer Emergency Response Team

**CESG** UK Government's National Technical Authority for Information Assurance

**CiSP** Cyber-security Information Sharing Platform

**DCLG** Department for Communities and Local Government

**GCHQ** Government Communications Headquarters

**LGA** Local Government Association

**NLAWARP** National Local Authority Warning, Advice & Reporting Point

**NCCU** National Cyber Crime Unit

**NCSC** National Cyber Security Centre

**NCSS** National Cyber Security Strategy

**NCSP/NCSP#2** National Cyber Security Programme / Second National Cyber Security Programme

**OCSIA** Office of Cyber Security and Information Assurance

**PSN** Public Service Network

**RCCU** Regional Cyber Crime Unit

**ROCU** Regional Organised Crime Unit

**SIRO** Senior Information Risk Owner

**SOCITM** Society of Information Technology Managers

**SOLACE** Society of Local Authority Chief Executives

**WARP** Warning, Advice and Reporting Points

ST GEORGE'S HOUSE

For more information about
Consultations at St George's House
visit www.stgeorgeshouse.org

St George's House, Windsor Castle, Windsor SL4 1NJ

T +44 (0)1753 848848 E house@stgeorges-windsor.org F +44 (0)1753 848849