techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

techUK Response

DSIT Software Vendors Call for Views

09/08/2024

About techUK

techUK represents the companies and technologies that are defining today, the world that we will live in tomorrow. The tech industry is creating jobs and growth across the UK. Over 1000 companies are members of techUK. Collectively they employ more than 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new and innovative start-ups. The majority of our members are small- and medium-sized businesses.

Executive Summary

Following the Call for Views on software resilience and security for businesses and organisations in 2023, techUK is pleased to see the government's commitment to building cyber resilience across the UK and we welcome and share government's ambition to improve the resilience and security of software.

The cyber security threat landscape is constantly evolving, and cyber-attack techniques are becoming ever more sophisticated, therefore, the security and resilience of software needs to evolve at an even greater pace to combat these threats. techUK supports government's efforts as they continue to explore which software risk areas should be prioritised for businesses and organisations, as well as how it can support the mitigation of those risks; and we are pleased to have the opportunity to respond to this Call for Views.

It should be noted that techUK is responding to this Call for Views on behalf of its members. Rather than answering each question set out in the consultation document individually, this response takes a thematic approach, addressing the key points that we would like to make regarding each part of the Call for Views, taking account of industry's views on the importance and dependency on software development.

The draft Code of Practice for Software Vendors (the 'Code') is an important document which can help to drive forward best practices across the software landscape, and members agreed that the principles outlined are a step forward in ensuring organisations are securing their software. Members agreed that the guidance should be a Code of Practice and not a 'standard' and would like to see this reflected in the terminology used throughout the document, avoiding 'requirements' and using the definition from BS0 of British Standards Institute (BSI). Work to operationalise the Code must use existing standards and the associate guidance to avoid creating barriers and fragmenting the skills base, particularly for small- to medium-sized enterprises (SMEs). To ensure there is good uptake of the cyber security principles, government must continue to work with industry to promote the education and awareness of its importance.

The shortage of cyber-specific personnel and the lack of awareness about required skills were a significant concern to members. With members promoting the importance of continued collaboration between government and industry as an essential tool to build the necessary skills base, ensuring supplier diligence and best practices across all organisations.

Members also highlighted the risk that the Code could become a bureaucratic tick-box exercise, particularly burdening SMEs. To remedy this, the government should ensure the Code drives best practices without increasing the burden on organisations and as code restricted to substitutable recommendations so that it can work across multiple contexts of use and maximise compatibility with existing standards. The government should recognise that commercial incentives for software quality are already significant, and members' reputations and market value depend on this. Raising awareness about the importance of best practices are crucial to level up the sector, spread best practice to inhouse software for non-software specialists and support due diligence in procurement. An appropriate Code that does not undermine existing standards that represent an international consensus, including the UK, of best practice may well have a role to play. Members also highlighted the need for procurement measures that relate to the value delivered and the importance of producing higher quality software across the supply chain.

As techUK has noted in the response to the Call for Views on the Cyber Security of AI Code of Practice, the last few years have been particularly busy in the policy space, for both the cyber security sector and the wider technology industry in the UK. Even larger digital companies with their own dedicated public affairs and policy teams have faced capacity challenges with the volume of policy proposals to provide feedback on. In addition to this, and while we appreciate matters were out of officials' control, the announcement of the General Election, the engagement restrictions inherent with the pre-election period, attention turning to the new government announcing the Cyber Security and Resilience Bill and the summer break, have also presented engagement challenges within the timeline given for responses to the Call for Views.

techUK recognises that similar challenges have faced government colleagues at a time when the communication of how various current and proposed codes of practice overlap was crucial. techUK, therefore, believes that more work is needed to clarify how the cyber security codes of practices align, as well as how the draft Cyber Security of AI Code of Practice complements this Code and other existing industry standards and recommendations. Indeed, members have raised concerns about the disconnect between different Codes and the principles the government expects industry to meet, which creates ambiguity and inconsistencies. We would, therefore, strongly recommend that more engagement takes place once government has published its response to this Call for Views.

In terms of the specific text comments, these should be taken as indicative and as an example of the issues and not an in-depth line by line analysis. Such a Call for Views should be done for any such documents containing requirements and acting as a standard. This however requires the proper WTO TBT Annex 3 compliant policies, governance and formats as used by standards bodies including BSI to be in place. In particular it requires clear IPR policies, publication, maintenance and transparency policies, comment resolution processes, line numbered documents and accountable editors to be in place.

techUK is eager to facilitate continued engagement between DSIT and those companies already doing significant work in this space, both in the UK and internationally, to support government's efforts to raise the bar across the whole software industry and build a more harmonised approach to software resilience.

Section 1 - Format and Target Audience

Organisational Engagement

Members expressed concern about the lack of clarity in the government's language throughout the Code. It is crucial for the government to clearly define what constitutes 'good' cyber security, as vague definitions could prevent organisations from properly adopting the Code's principles.

Members agreed that the document should be a Code of Practice and not a 'standard' and should therefore avoid using terms like 'mandate' or 'requirement' which would confuse the purpose of the document. When detailed 'mandated' technical controls appear overly prescriptive, the Code risks becoming narrow and un-relatable or unworkable to organisations working outside of the security sector or in differing contexts especially medical, telecoms, aerospace and defence and safety critical systems.

To improve the uptake of the Code, the government should use language that resonates with industry. The Code suggests that responsibility for implementing the principles lies with the senior responsible officer in a software company. However, in practice, responsibilities are distributed differently across organisations, and it's crucial for the government to recognise that there is no one-size-fits-all approach. Members also pointed out inconsistencies in the terminology used, such as referring to NIST standards as "secure by default." The term "accessible" can have specific meanings in software, so the government should clarify that it refers to the way information is shared with customers rather than broader accessibility issues. There is also a need for clarity on what is meant by "technical controls." Consistency in language is vital for alignment between the Code and the industry's common practices.

The government should not introduce new language in the Code, rather they should refer to the legal and contractual terminology. One Member highlighted this in Principle 4.3 where the Member recommended that the language be changed to '*Where notable incidents may cause significant impact to customer organisations, ensure information is made available to customers in a manner compatible with legal obligations*'. Members also highlighted the need to edit the language in Principle 4.5 to read 'Ensure that the organisation proactively supports affected customers during and following a cyber security incident to contain and mitigate the impacts of an incident.' This is due to the need to have a centralised approach to cyber security and incident management practices. If a customer-by customer approach is used, this can become cumbersome for SMEs and can create cost barriers which can impact on the effectiveness of the process.

Members also expressed concern over the use of 'shall' and talking about requirements organisations would be expected to meet when aligning themselves with the Code, as this will cause consistency issues with actual standards subject to accredited certification.

Throughout the Code, the 'Senior Responsible Officer' is referenced as the individual responsible for implementing the Code and subsequent principles. Members shared concerns that this terminology would not resonate with mature organisations who follow recognised international standards and have recognised roles and governance structures which assign ownership and responsibility for these matters. It is also not reflective of the language used by industry as it is public sector specific. If the aim is to promote a culture of individual accountability within an organisation, then this language should be changed to reflect the objective. More clarity should be given to the individual or group of individuals who would be held accountable for implementing the Code within an organisation.

Members were also concerned about references to 'model contractual clauses' as this could imply that commercial compliance exercises will be used which would not directly increase the cyber resilience of software vendors and lead to an over reliance on tick box compliance rather than procurement due diligence. Overall, members stressed that this level of detail does not belong in a principle led Code or in implementation guidance. Members recommended that the government refer to standards and guidance produced by the BSI. The government should also refer to international standards which represent the international consensus on best practice.

Section 2 - Barriers to Implementation

Guidance and Standards

techUK members broadly agree with the statements outlined in the Call for Views. However, they questioned the appropriateness of the government producing guidance and standards, which are typically developed by bodies such as the British Standards Institution (BSI). Members felt that more clarity is needed on the long-term purpose of the Code, as ambiguity around its purpose could hinder organisational uptake. They also agreed that the government should support organisations in adopting 'secure by design' principles, and that this support should be tailored for small to medium-sized enterprises (SMEs) predominantly focused on developing much needed skills and supporting international standards to support and enable UK exports and trade.

There is potentially a need to establish guiding principles and communicate that to Boards and SME leaders, especially those not predominantly in the software sector, and if strictly kept to that scope this Code could support these individuals. While the guidance referring to exact standards would benefit small companies and software organisations aiming to improve their offerings, national and multinational organisations already adhere to international standards for software.

In regards to the first statement, members raised concerns about how government departments manage their own infrastructure as successful cyber-attacks are often partly due to weak infrastructure. The government should lead by example, yet members have noted that government departments frequently use technology that does not meet the highest security standards needed to protect organisations from an attack.

Members also highlighted the lack of consistency and coherence between previously published Codes of Practice, including the Technology Code of Practice, the recently consulted Cyber Governance Code of Practice, and the currently reviewed Cyber Security of AI Code of Practice. techUK members are concerned about the disconnect between these different Codes and the principles the government expects industry to meet, which creates ambiguity. Additionally, there is concern about the burden this places on various sectors. Companies may need to allocate more resources to comply with these principles, detracting from their research, development, and innovation efforts in the cyber security space. Many techUK members also worry that these Codes will create additional bureaucracies that hinder sector growth. These issues are particularly significant for SMEs, which often lack the funding and capacity to implement the numerous principles outlined in the Code.

It has also been noted that the overlap between secure AI and secure software is total: creating and deploying AI is creating and deploying software. While there are specific additional AI risks and controls, the Software Vendors Code of Practice should in effect be a subset of the Cyber Security of AI Code of Practice. However, the two codes as presented are almost completely different from the principles on down. There must be a clear and simple way to use both simultaneously and yet as presented that would be a significant effort. This underlines the risks of going beyond codes of practice and into requirements where these are described differently as an extensive effort would have to be undertaken to approach them simultaneously to the other standards like ISO/IEC 27001 and NIST that are absolutely required by the market.

techUK and its members broadly agree with the principles outlined in the Code, recognising that they address critical areas for software vendors to focus on to ensure systems are built using secure-by-design principles. However, there is concern that the Code overlaps into standards and has details that only work in specific context, which does not recognise the tensions that already exist between engineering objectives. Detailed guidance is needed for industry to operationalise these principles correctly, this guidance should refer to extant standards including the general ISO IEC 27001 and 27002 and the software specific ISO/IEC 27034.These provide clear, actionable steps that organisations need to follow to support a continuous process of security and resilience adapting to the changing threats and should be supported not undermined.

In particular on principle 2.3 members highlighted that there are a number of principles that already exist around trust and given the plain English meaning of the word, it's meaning in the Code is currently unclear. Members also expressed concern that the Code does not reflect the holistic nature of software resilience, which was originally outlined by industry during the first consultation in 2023.

Although the Code is voluntary, the government should focus on how it will be adopted by industry. Often, when such documents are published, the timeline for adoption is very short. The government should consider the time and cost required for industry to implement these principles. It is especially important for SMEs, which often lack the resources and funding needed to implement new guidance. Setting realistic timeframes is essential to avoid creating barriers that could hinder sector growth.

Furthermore, should the same path be taken as with other codes of practice – when certain principles of a voluntary code eventually became mandated through regulation (for example, such as the Product Security & Telecommunications Infrastructure Act) – the timescale can be significant (approximately 8 years in that case). There is, therefore – and whatever the outcome of this Call for Views – a clear and pressing need to instigate an education and awareness effort to promote the principles that are contained in the draft Code. However, we would emphasise that the objective is key, recognising the extant international standards and skills shortage. A focus on implementation and uptake of the Code as is, would be counterproductive and could be perceived as protectionist.

Cyber Skills

Members raised concerns about the skillset required for implementation, especially for SMEs facing capacity and funding limitations. There is a critical shortage of cyber-specific personnel with the necessary qualifications and technical expertise. Additionally, there is a lack of awareness across organisations about the skills needed to implement the principles outlined in the Code.

To address these challenges, the government and industry should collaborate to develop the skills needed for operationalising the Code via best practice contained in actual standards. This collaboration will ensure supplier diligence is recognised by both software suppliers and organisations more broadly. Building a strong skills base in the market is essential to create best practices applicable to organisations of all types.

International alignment

A general theme members highlighted was the lack of international cohesion between the Code and activity which has been carried out by international counterparts. Given the global nature of software supply chains, with a particular focus on assurance and trade agreements, DSIT should engage with the Department for Business and Trade and the work they have already done and are continuing to do in this space.

There are a number of evolving regulatory pieces which the government should be aware of. In particular, work carried out by counterparts in Europe and the US should be aligned with accordingly. One techUK member highlighted the importance of aligning with guidance on ransomware developed by the US Cybersecurity and Infrastructure Security Agency (CISA). This guidance ensures organisations are appropriately prepared for a ransomware attack by aligning with specific measures outlined in the guidance.

Building on this, members highlighted the promotion of the use of NIST's Secure Software Development Framework (SSDF), which a US standards committee (INCITS) is converting to a national (ANSI) standard that can be fast tracked as an international (ISO/IEC JTC1) standard. The NIST SSDF takes a risk-based approach to secure software development and incorporates feedback from many stakeholders and experts, including civil society and industry.[1] Adopting SSDF as a model for secure software development in the UK will help promote harmonisation of U.S. and UK secure software development practices, which will hopefully be a starting point for further international harmonisation.

Procurement Barriers

Members expressed concern that the Code places significant onus on the supplier and stressed the importance of creating balance in procurement and how procurement will measure and value the adoption of the Code or equivalents.

There is a risk that the Code could be viewed as a tick-box exercise which is only implemented by government organisations, which would only add bureaucracy into the system and could hinder best practices. It could also create a disproportionately competitive environment, burdening only SMEs who do not have the ability to dedicate the resources needed to review more guidance.

Members suggested the government consider how the Code can drive best practice across industry, without increasing a burden on organisations responding to government contracts. One member suggested introducing continuous assurance activities, undertaken by a third party, where the risk profile dictates. This would encourage meaningful adoption of the Code. Members also suggested the government should review the work international counterparts have undertaken to remove this burden and foster productive change.

In the absence of tangible/certified best practice the government should provide commercial incentives for organisations to adopt nationalist approaches and consider the measures used to encourage compliance with the Code and allow equivalents and extant standards. It

[1] ANSI (2024) 'Projection Initiation Notification System (PINS)
https://share.ansi.org/Shared%20Documents/Standards%20Action/2024-PDFs/SAV5505.pdf

is also important that the government raise awareness of the importance of adopting best practices, to ensure there is a good uptake of cyber security principles regardless of the Code. Organisations must be aware of the risks and liabilities associated with not protecting the software and supply chains.

Contractual clauses often fail to clearly relate to the value they deliver, and the government must assess whether the Code will generate the desired value or add bureaucratic layers without achieving the necessary outcomes. Members agreed that higher quality software throughout the supply chain is an important step to achieving best practice and that the maturity of these practices is crucial to fostering an environment which results in this objective.

Some members have highlighted the need to tread very carefully with certification because it can quickly become a tick-box exercise; and trying to produce a set of repeatable, measurable, certification measures will be difficult in a sector where organisations do things in different ways. Furthermore, caution should be exercised if it were to be UK accreditation as opposed to international certification. Members suggested that guidance should be tailored to the size of the organisations, for example SMEs could be encouraged to meet specific areas of guidance, or aim these types of organisations to more general principles such as those promoted on the National Cyber Security Centre (NCSC) website.

One argument for certification of software above certification of organisation is that companies tend to buy specific software; however, it has also been pointed out that this would be difficult as it would need to be version based (and re-certified every time there was a patch), and certification schemes are often slow and would be likely not keep pace with the time it takes to develop the software, which could result in the a situation whereby software is being certified and preserved beyond its security ‘shelf life’. Therefore, it would rather need to certify the support model of the software. However, one member noted that it could also be argued that the current speed of some software patch/fix development and release (with zero awareness of the risk by the users until released) is not at sufficient speed to effectively address known vulnerabilities.

Responsibility to implement the Code

For non-software organisations within the scope of the Code, the Code assumes a context of software resilience and enterprise IT. In particular the more specific and quite detailed ‘mandated’ technical controls appear overly prescriptive for all possible contexts. Members suggested clarifying that organisations in different industries should apply the Code according to their specific contexts. This will help ensure a broad range of industries understand how to implement the principles effectively. It is important for the government to contextualize the baseline requirements so that all organisations, whether they are software vendors or not, can operationalize the guidance using context relevant standards.

There needs to be a clearer distinction between the product/service and the organisations responsible for ensuring high levels of security within software vendors. Different products within a company may require distinct risk assessments, carried out by various personnel. While it is important for the principles to address multiple areas, there is a notable lack of focus on risk mitigation, applied using controls from people processes, and technology. ISO 27001, for example, provides a framework that allows organisations to operationalise its standards, but the Code is missing points on validation, feedback, risk mitigation and risk assessment.

While not referenced in the Code, Members suggested reviewing the resilience of supply chains alongside the resilience of Cyber Security and other areas. It is important that the cyber security approach includes measures to support continuous improvement. Members suggested an improvement matrix should support cyber resilience to ensure organisations can measure against. Organisations should have contingency plans in place to ensure there is sufficient contingencies to respond appropriately.

Members also highlighted the importance of considering the efficacy of the standards, if there is a good uptake of the standards that should be recognised as compliance with the Code where necessary. The Code should be well evidenced by what works and what doesn't work in regard to outcomes. This should be made publicly available across vendors in a neutral way.

As regulatory approaches on this topic and related issues continues to evolve around the world, techUK members would encourage the government to remain engaged with international partners and continue to build its role as an international leader on this important issue, as a well-informed regulatory approach will enable organisations to respond well to changing security threats.

Further points for consideration

One member suggested exploring the impact the Computer Misuse Act 1990 (the CMA) has on Software Vendors. Members agree that we need an effective legislative and regulatory and standards environment to protect citizens by making the UK the safest place to live and work online, and to prosecute and dis-incentivise bad actors. An additional advantage in conducting a review and update of the CMA would be to look for opportunities where government could address ambiguities in the law that might not address the latest tools and techniques used by industry, academia and the research community in securing our digital ecosystem. Some of these issues are indeed contentious, but government and industry can continue to collaborate towards shared ambitions. techUK has offered our continued support in informing the review of the legislation in order to create a better business environment that supports the growth of the UK's cyber ecosystem.

More broadly on the Call for Views itself, while techUK welcomes government's commitment to improving information sharing between software vendors and their customers, the timing of the consultation has been problematic. While we completely appreciate that events have been out with the control of officials – such as the announcement of the General Election;

the pre-election period when engagement with industry was unable to take place; and uncertainty around whether the Call for Views would be granted approval to continue from the new Minister; as well as the clash with summer holidays – it has been more difficult for techUK to engage as many members as usual on this Call for Views. We would, therefore, strongly recommend that more engagement takes place once government has published its response.

techUK recognises that similar challenges have faced government colleagues at a time when the communication of how various current and proposed codes of practice overlap was crucial. techUK, therefore, believes that more work is needed to clarify how the cyber security codes of practices align, as well as how the draft Code of Practice for Software Vendors complements them and other existing industry standards and recommendations. Indeed, members have raised concerns about the disconnect between different Codes and the principles the government expects industry to meet, which creates ambiguity. Additionally, there is concern about the burden that this could place on various sectors and potential hinderance of sector growth. These issues are particularly significant for SMEs, so consideration should be given to what support they should be given to help their compliance to the codes.

We would, therefore, strongly recommend that more engagement takes place once government has published its response to this Call for Views and techUK stands ready to support and facilitate this engagement.