Cybersecurity
Coalition

July 11, 2021

*Submitted via email to cyber-review@dcms.gov.uk*

Cyber Resilience Team - 4/47
DCMS
100 Parliament Street
London
SW1A 2BQ

**RE: Call for Views on Supply Chain Cyber Security and Managed Service Providers**

The Cybersecurity Coalition ("the Coalition") submits this comment in response to the call for views launched by the Department for Digital, Culture, Media and Sport ("DCMS") on supply chain cybersecurity. The Coalition appreciates the opportunity to comment on the call for views and looks forward to working with the Government to establish a robust approach to supply chain cybersecurity.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services. We are dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management.

The Coalition commends the Government's proactive efforts to drive a coordinated approach to this critical area of cyber risk management. As leaders in the cybersecurity industry, we recognise the importance of securing digital supply chains, and the challenges of doing so in an effective manner. In its current form, however, we are concerned that the proposed approach will not be effective for two reasons.

Firstly, under the current definition of Managed Service Providers ("MSPs"), a very large proportion of technology companies could be considered in scope.

> *A supplier that delivers a portfolio of IT services to business customers via ongoing support and active administration, all of which are typically underpinned by a Service Level Agreement. A Managed Service Provider may provide their own Managed Services, or offer their own services in conjunction with other IT providers' services. The Managed Services might include: Cloud computing services; Workplace*

*services; Managed Network; Consulting; Security services; Outsourcing; Service Integration and Management; Software Resale; Software Engineering; Analytics and Artificial Intelligence (AI); Business Continuity; and Disaster Recovery services.*

Drawing such a broad scope will:

1. Create a lack of clarity for organisations, many of whom are SMEs, regarding the legal and cybersecurity obligations that they must meet;
2. Lead to inconsistent compliance, as organisations take a 'best guess' as to whether and how they need to comply;
3. Inhibit the ability of companies and their regulators to take a risk-based approach at both a sectoral and company level. Inevitably this leads to wasted resources by industry and government entities, who are often working with limited resources, undermining security efforts overall; and
4. Require companies to implement security measures that are neither reasonable, nor proportionate to the risks faced by their business. Setting a baseline to cover too broad a range of businesses will present smaller, less mature organisations with a standard that they cannot possibly meet and/or set the baseline too low for larger, more mature organisation. Neither outcome benefits the overall security environment.

Secondly, the intended regulatory outcome is not clearly defined. The term "supply chain cyber security" is used to address myriad security risks, real or perceived. In this instance, it is not clear whether the intent of the proposal is to:

- Ensure that MSPs have adequate *internal* security practices and appropriate end-to-end risk management processes given the breadth of clients that they are collectively serving; or
- Ensure that MSPs are sufficiently vetting/maintaining a sufficient cybersecurity baseline across *their* supply chain.

An understanding of the government's intent is critical to determining the most effective approach to achieving it. For its Telecommunications Security Requirements, for instance, the Government opted to place only Internet Service Providers ("ISPs") and Mobile Service Providers (MSPs) in scope, developing a separate Vendor Assessment for their suppliers. The Vendor Assessment addresses potential risks in the supply chains of ISPs and ensure that supply chain risks are addressed in a manner appropriate to the risk. The Government's approach is the right one, given the different risk profile and security requirements of ISPs and their vendors.

We would welcome further clarification from the government in these two areas. With a better understanding of the Government's objective and scope, we can provide more useful feedback with regards to the most effective approach to achieving them. In the interim, we have provided feedback to those questions in Part 1 of the Call for Views which are applicable to our industry associations.

We appreciate the opportunity to participate in the Government's Call for Views. As the conversation around this topic continues to evolve, we would welcome the opportunity to further serve as a resource on both technical and policy questions to ensure that the resulting proposal is effective in improving the U.K.'s supply chain cybersecurity risk management.

Respectfully Submitted,
The Cybersecurity Coalition

July 11, 2021

CC: Ari Schwartz, Venable LLP
Alex Botting, Venable LLP

**Questions on barriers to effective supplier risk management:**

1. How much of a barrier do you think each of the following are to effective supplier cyber risk management?
    a. Low recognition of supplier risk – *Somewhat of a barrier*
    b. Limited visibility into supply chains – *Severe barrier*
    c. Insufficient expertise to evaluate supplier cyber risk – *Somewhat of a barrier*
    d. Insufficient tools or assurance mechanisms to evaluate supplier cyber risk – S*evere barrier*
    e. Limitations to taking action due to structural imbalance – *Don't know* (situation dependent)

2. Are there any additional barriers preventing organisations from effectively managing supplier cyber risk that have not been captured above?
    - *Yes*
    - No
    - Don't know

3. [If Yes] What additional barriers preventing organisations from effectively managing their supplier risk are you aware of?

    *Organisations, particularly those that outsource certain cybersecurity audit and assessment functions, may not have sufficient resources or skills in-house to be able to assess those companies that they retain. Indeed, they may outsource such functions precisely to avoid the need to bring such capabilities in-house.*

    *In such instances, organisations can leverage international standards for supply chain risk management evaluation such as ISO 27701 and 28000, which give them an objective benchmark against which to assess prospective vendors. Broader awareness and use of such standards would benefit the ecosystem by reducing asymmetry of information caused by resource/skills constraints.*

**Questions on supply chain cyber risk management**

4. Have you used the NCSC's Supply Chain Security Guidance?

    *Some of our members have, some have not.*

5. How challenging do (or would) organisations find it to effectively act on these principles of supply chain cyber risk management, as outlined in the NCSC's Supply Chain Security Guidance?

    a. Understanding the risks - *Very challenging*
    b. Establishing control - *Very challenging*
    *c.* Checking arrangements - *Slightly challenging*
    *d.* Continuing to improve, evolve and maintain security - *Very challenging*

6. What are examples of good practice for organisations implementing these aspects of supply chain cyber risk management?

    *See the Coalition's comments in the introduction, regarding the need for the Government to define what aspects of supply chain cyber risk management it is referring to in this context.*

7. What additional principles or advice should be included when considering supply chain cyber risk management?

    *See the Coalition's comments in the introduction, regarding the need for the Government to define what aspects of supply chain cyber risk management it is referring to in this context. In terms of general practices, process-focused assessments, continual service improvements and ongoing risk analysis are critical to effective risk management. Approaches that focus on end-to-end risk management should be promoted, including those that identify supply chain risks across product lifecycles. Given the shifting nature of both the cyber threat landscape and MSPs' digital infrastructure, static compliance regimes are ill-suited to meet the risk management needs and undermine efforts aimed a consistent improvement.*

**Questions on supplier assurance**

8. Have you used or do you plan to use the NCSC's Supplier Assurance Questions?

    *Some of our members have, some have not.*

9. Since publishing the NCSC's Supplier Assurance Questions, it has been noted that the guidance could also cover the use of supplier-provided apps (e.g. where a supplier requires use of apps on an organisation's network to deliver its service to that organisation). Are there any additional areas of supplier assurance that should be outlined?

    - Yes

- No
- *Don’t Know*

10. What additional areas of supplier assurance should be outlined?

*Our response to question 7 sets out good practices that organisations should implement.*

Questions on commercial offerings:

11. How effective are the following commercial offerings for managing a supplier’s cyber risk?
    a. Private supplier assurance - *Somewhat effective*
    b. Platforms for supporting supplier risk - *Somewhat effective*
    c. Supply chain management system providers - *Somewhat effective*
    d. Risk, supply chain and management consultancies - *Somewhat effective*
    e. Suppliers of outsourced procurement services - *Somewhat effective*
    f. Industry cyber security certification schemes - *Very effective*

12. What additional commercial offerings, not listed above, are effective in supporting organisations with supplier risk management?

    *The challenge with using commercial offerings as a tool for managing supplier risk is that it transfers the risk to a third party or relies on the contractual risk management model. As a result, the risk to the broader ecosystem is not necessarily mitigated. Commercial offerings can nevertheless provide a useful tool to support an organisation's risk management processes, but that should not replace the need for the organisation to understand their own risk posture and apply the relevant principles or security guidance.*

    *International standards (including ISO28000 and ISO 27701) are a key tool that organisations should leverage to understand their supply chain risks. Such standards can also provide a consistent measure of conformance and provide organisations with some level of assurance as to the suitability and commitment of a particular vendor.*

**Question on additional government support:**

13. How effective would the following government actions be in supporting and incentivising organisations to manage supply chain cyber risk?

a. Awareness raising of the importance of supply chain cyber risk management through the use of campaigns and industry engagement - *Somewhat effective*

b. Additional support to help organisations to know what to do, such as:
   - Improved or additional advice and guidance - *Somewhat effective*
   - A tool that draws on existing advice and standards to help organisations manage supplier cyber risk - *Somewhat effective*

c. Providing a specific supplier risk management standard that:
   - Outlines minimum and good practice and/ or - *Somewhat effective*
   - Provides assurance that an organisation is managing their supply chain cyber risk - *Very effective*

*d.* Targeted funding to help stimulate innovation and grow commercial offerings that support organisations with their supplier risk management (e.g. Government competitions, accelerator programmes) - *Somewhat effective*

   a) Regulation to make procuring organisations more responsible for their supplier risk management.- *Very effective*

   b) Other (Please specify) – *N/A*