Ministry of Defence

Paul Lincoln
Second Permanent Secretary, MOD

Charlie Forte
DG Chief Information Officer, MOD

Andrew Forzani
DG Commercial, MOD

Ministry of Defence Main Building
Whitehall
London
SW1A 2HB

Defence Industry CEOs/Defence Leads

18 Dec 24

Driving Cyber Resilience in the Supply Chain – Call for action

As you are aware, Cyber security remains one of the greatest threats we face as a Defence enterprise, with the global threat landscape intensifying over the past year. It is vital we are resilient to ensure we continue to collectively deliver critical Defence capabilities.

We have previously written out individually to companies in the Defence supply chain to encourage improvements in cyber resilience. However, a number of incidents this year within the public sector supply chain serve as a stark reminder of the need for robust and continuous enhancement of our cyber security measures.

Irrespective of the nature of your business, building resilience and good security practice across the end-to-end supply chain to mitigate this risk is non-negotiable and a critical requirement for all contracts with the Ministry of Defence. Mounting an effective cyber defence is complicated and the nature of the measures you need to take are driven by multiple factors. However, the National Cyber Security Centre (NCSC) has produced clear guidance and advice. We are therefore writing to highlight this guidance and lay out our expectations.

What are we asking you to do?

Review Your Organisation performance against the NCSC's Cyber Assessment Framework. The NCSC has developed the Cyber Assessment Framework[1] to aid you in developing a robust cyber defence. The Framework is supported by a series of indicators of good practice, and we would expect to see you achieving these standards. All elements of the Framework are important but we would like to draw your attention to the following areas:

- **Govern** – Your organisation must have appropriate management policies, processes and procedures in place to govern its approach to the security of network and information systems. You should be holding regular board-level discussions on the security of the network and information systems supporting the operation of your essential functions and these should be informed by expert guidance.

- **Identify** – You must ensure that your organisation understands, documents and manages access to the networks and information systems that support the operation of your essential functions. Users, and automated functions, that can access data or services must be appropriately verified, authenticated and authorised.

- **Protect** – Your organisation must define, implement, communicate and enforce appropriate policies, processes and procedures to secure and proactively patch the systems that support your essential functions.

[1] Cyber Assessment Framework - NCSC.GOV.UK

- **Detect** – You must ensure that your organisation has the capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.

- **Respond and Recover** – You must have well-defined and tested incident management processes in place, to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.

Adopt Active Cyber Defence (ACD). Register your company on the MyNCSC portal[2] and prioritise the adoption of ACD tools, including the "Early Warning" service.

Implement the new Cyber Security Standard for Suppliers.[3] We have recently published an enhanced standard for organisational cyber resilience that we will require all supply chain organisations to apply in the coming months.

Deliver 'Secure by Design' Continue to apply MOD's through-life approach to development of products, systems and services. By designing security into projects from the start, you help Defence stay ahead of adversaries and maintain national security.

Forward look

MOD is making significant investment in order to transform the way in which risk is managed in the end-to-end Defence supply chain, including enhancing cyber security.

You are hopefully already familiar with MOD's **Cyber Security Model (CSM) -** a new risk-based methodology to enhance supply chain resilience, underpinned by the enhanced standard for supply chain organisations. This is being rolled out across the supply chain as part of our enhanced approach to assurance.

We are also working with NCSC colleagues regarding its central offering of **ACD** services and progression of such under ACD2.0, promoting access to a range of tools and services to Defence supply chain organisations to help further reduce the harm from commodity cyber-attacks.

Accessed via the MyNCSC portal, registered Defence suppliers will be among the first to learn about, and have access to, new services as they evolve.

We will also be establishing new collaborative fora, such as via the '**Connect, Inform, Share, Protect**' (CISP)[4] portal, alongside other activities, with further details to be published on such in the coming months – sharing threat intelligence more effectively across organisational boundaries and working together to 'defend as one'.

We ask that you cascade this letter to all Defence subcontracts that you may hold.

Thank you for your continued support and ongoing engagement; this remains vital in safeguarding the UK's Defence and national security, ensuring we can operate effectively in times of crisis. We know you wish to join us in ensuring that we keep pace with the threat and keep us secure.

Yours faithfully,

Paul Lincoln
Second Permanent Secretary
MOD

Charles Forte
DG CIO
MOD

Andrew Forzani
DG Commercial
MOD

[2] https://my.ncsc.gov.uk/

[3] Defence_Standard_05-138__Issue_4_-_cyber_security_for_defence_suppliers.pdf (publishing.service.gov.uk)

[4] https://www.ncsc.gov.uk/cisp/home