Notice to Suppliers

Supply Chain Security: Building Resilience

Originator: Kaveh Pourteymour
Job Title: Group Chief Digital & Information Officer (CDIO)
Business Unit: All

NTS Number: NTS_628
Issue: 1
Date: 17 May 2025

Scope/Applicability: All Rolls-Royce suppliers and partners

Dear Supplier,

You will be aware that the global cyber security threat landscape is rapidly evolving. We must collectively take action to protect our critical capabilities and supply chains and reaffirm our commitment to robust and continuous improvement of cyber security measures.

Building resilience and good security practice across the end-to-end supply chain to mitigate this risk is non-negotiable; it is a critical requirement for safety, and for demonstrating compliance to customer contracts and regulations. Rolls-Royce adheres to customer and regulatory cyber security requirements and wants to ensure that our suppliers and partners do the same.

The purpose of this NTS is to emphasise the importance of enhancing your organisation's cyber defences and ensure continued compliance with Rolls-Royce and customer and regulatory cyber security requirements.

Action Required:

To ensure your organisation is aware of the importance of safeguarding the supply chain, and prepared to enhance your cyber security, we require suppliers to take the following actions:

1. **Review your organisation's performance against cyber security requirements**

   To assess compliance and identify areas of improvement, use Rolls-Royce Supplier Minimum Cyber Security Standard [Ref 1], and if applicable, defence flow down requirements:

   - For US Department of Defense (DoD) suppliers, use the CMMC compliance guide. [Ref 2]
   - For compliance with UK MOD Cyber Security Model, see the MOD cyber security requirements guide [Ref 3]

2. **Update your cyber incident response plans**

   If a cyber incident impacts Rolls-Royce data, goods or services, you must comply with Section A 1.7 of the Rolls-Royce Supplier Minimum Cyber Security Standard [Ref 1]. Add the email address(es) for reporting incidents to Rolls-Royce SOC to your cyber incident response plans.

   The following advice and guidance can help you with a Cyber Incident Support Plan:
   - Rolls-Royce cyber security experts offer advice, guidance and best practices: Supply chain incident response webinar [Ref 4] and toolkit [Ref 5]
   - The UK National Cyber Security Centre (NCSC) provides guidance on the benefits and steps for creating and testing your Incident Response Plans (Incident management - NCSC.GOV.UK)

[Ref 6], with specific advice for your Board Members (Planning your response to cyber incidents - NCSC.GOV.UK) [Ref7]

- US Cybersecurity and Infrastructure Security Agency (CISA) offers guidance and assistance for US businesses to plan and recover from cyber incidents (Cyber Incident Response | CISA) [Ref 8], and useful playbooks to help you get started (Federal Government Cybersecurity Incident and Vulnerability Response Playbooks (cisa.gov) [Ref 9]

3. Sign up to the Rolls-Royce Supplier Cyber Newsletter

To stay informed on updates and best practices, we encourage you to subscribe to our monthly newsletter by registering here: Cyber Security | Rolls-Royce [Ref 10] or Register here

Thank you for your continued cooperation. If you have any questions, please get in touch with your usual Rolls-Royce point of contact.

NTS Category:	**Authorised by:**
General Information	Kaveh Pourteymour Group Chief Digital & Information Officer (CDIO)

Ref 1: https://cte.suppliers.rolls-royce.com/GSPWeb/ShowProperty?nodePath=/BEA%20Repository/Global%20Supplier%20Portal/Section%20DocLink%20Lists/Supplier%20training/Cyber%20Security%20Requirements/Column%201/Section%201/Documents/Minimum%20Cyber%20Security%20Standard//file

Ref 2: dod-cyber-security-compliance guidance-2024.pdf

Ref 3: mod-cyber-security-requirements-2025.pdf

Ref 4: https://www.rolls-royce.com/sustainability/cyber-security.aspx#section-webinars

Ref 5: https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/sustainability/Supplier-docs/cyber-security-incident-response-guidance-resource.pdf

Ref 6: https://www.ncsc.gov.uk/collection/10-steps/incident-management

Ref 7: https://www.ncsc.gov.uk/collection/board-toolkit/planning-your-response-to-cyber-incidents

Ref 8: https://www.cisa.gov/cyber-incident-response

Ref 9: https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Ref 10: https://www.rolls-royce.com/sustainability/cyber-security.aspx#/