Notice to Suppliers

Rolls-Royce Supplier Cyber Security Standards

Originator: David Loseby
Job Title: Director of Procurement, Group
Business Unit: All

NTS Number: 523
Issue: 1
Date: 19th December 2020

For the attention of the Managing Director

Scope/Applicability:

All Rolls-Royce plc suppliers.

Dear Supplier,

Introduction:

There is an increasing body of research that demonstrates that malicious groups are actively targeting manufacturing and defence organisations by gaining a foothold in to their supplier' systems causing possible financial and reputational damage, product safety issues and operational disruption.

Rolls-Royce places great importance on protecting the confidentiality, integrity and availability of its data and information systems. Due to the ever-evolving threat landscape, increasing supply chain complexity and regulatory pressure, it is our responsibility to implement measures to control, manage and enhance the security within our supply chain system.

As part of those measures, Rolls-Royce will be introducing a supply chain cyber security risk management process from January 2021. This process will require our suppliers to adhere to a set of cyber security standards, which will be determined on a supplier impact assessment and will include the ongoing monitoring of compliance through continuous assurance tooling.

There will be two cyber security standards, the **Rolls-Royce Supplier Baseline Cyber Security Standard** and the **Rolls-Royce Supplier Enhanced Cyber Security Standard**, which are accessible on the Global Supplier Portal. The results of the impact assessment will enable Rolls-Royce to determine the most appropriate cyber security standard that best suits the suppliers risk profile, for example, a supplier of strategic importance or a supplier handling highly confidential Rolls-Royce data will warrant a greater level of cyber security maturity and compliance with the Rolls-Royce Supplier Enhanced Cyber Security Standard.

Where suppliers can demonstrate current certification to a national Defence cyber security standard (NIST 800-171, CMMC Level 2 or higher or Defence Standard 05-138 'Very Low' profile or higher), and the certification scope covers the Rolls-Royce contractual scope, the Rolls-Royce cyber security standards will not apply.

What action to take:

The applicable cyber security standard will be applied to all new and existing contracts. During Q1 2021, Rolls-Royce will share targeted communications outlining how the applicable cyber security standard will be introduced and the supporting compliance management process. In the interim, the cyber security standards are available on the Global Supplier Portal for you as suppliers to familiarise yourselves with the requirements and provides an opportunity to self-assess levels of compliance.

To further support the supply chain cyber security risk management process, Rolls-Royce will introduce continuous assurance tools, such as a maturity-based questionnaire which will form the basis of periodic security reviews and enable the pro-active identification and resolution of cyber security issues where appropriate. These tools and questionnaires will offer greater efficiency and usability in comparison to the existing cyber security survey delivered through the Assent portal.

Conclusion;

As all companies are potential targets, working together to minimise the risk of cyber incursion is important. Threat actors are indiscriminate in their use of supply chains to access networks and therefore we would request that all our suppliers support us in preventing any malicious activity and immediately contact Rolls-Royce on UK.SOC@rolls-royce.com if you identify anything that causes you concern or suggests that anything untoward has occurred on your network.

If you have any questions generally about the mandated cyber security requirement then please send your questions to RRITSecurityCompliance@rolls-royce.com.

NTS Category:	**Authorised by:**
General Information / Communication	David Loseby Director of Procurement, Group