THALES

www.thalesgroup.com/uk

SECURE COMMUNICATIONS AND INFORMATION SYSTEMS

DEFENCE CYBER PROTECTION PARTNERSHIP

Becoming MOD Cyber-Ready

Help and support for suppliers to the Ministry of Defence.

SECURE COMMUNICATIONS AND INFORMATION SYSTEMS

DEFENCE CYBER PROTECTION PARTNERSHIP

Becoming MOD Cyber-Ready

HELP AND SUPPORT FOR SUPPLIERS TO THE MINISTRY OF DEFENCE

If you want to bid for contracts to supply the Ministry of Defence (MOD), you must first comply with its Cyber Security Model (CSM). Developed by the Defence Cyber Protection Partnership (DCPP), the purpose of CSM is to protect any 'MOD-identifiable information' that could be transferred during the contract.

There are several levels of compliance according to the risk profile of the contract and they apply to every part of the supply chain, from the largest prime to the smallest component manufacturer. The requirements for complying with each risk profile are set out in DEFCON 658.

THE JOURNEY TO COMPLIANCE

Although it is relatively easy to comply with the requirements for a low-risk contract, higher risk contracts can stipulate as many as 43 complex security controls which must be in place before the contact can start. These mandatory security controls are described in DEFSTAN 05-138.

It is important to understand that the DCPP's requirements are specific to the risk profile of each and every contract. Suppliers face disqualification if they cannot demonstrate compliance to each of the required security controls. Each supplier is responsible for its own compliance

Complex security controls, mandatory requirements, DCPP, CSM, DEFCON 658, DEFSTAN 05-138 - if all this sounds daunting, it's time to talk to Thales.

SHARING YOUR OBJECTIVES

A secure and mature supply chain supported by a wider pool of security-compliant suppliers is better for the MOD, better for Thales and better for you.

That's why are committed to promoting the importance of adopting a good cyber security culture which protects everyone from the real and present threat of cyber attacks.

EXPERTS IN THE DCPP'S CYBER SECURITY MODEL

As part of the working group that was tasked with developing the DCPP's CSM requirements, Thales knows exactly what it takes to achieve compliance with every security requirement at all levels from the lowest to the highest.

What's more, we continue to collaborate with the DCPP helping to bring about steady improvements to the security of the supply chain. And with a heritage of providing independent cyber security consultancy support in the most complex and security critical environments, Thales stands ready to help.

REDUCING COMPLEXITY

Suppliers who want to bid for a contract with the MOD are required to complete a Supplier Assurance Questionnaire (SAQ). Unfortunately, some SAQs pose more than 100 questions of varying complexity – a major challenge that can consume significant time and resources. But Thales can reduce this workload.

Everything we do is designed to bring clarity to what can be a complex and cumbersome process. Our experienced consultants will work with you to cut through the complexity of the DCPP CSM requirements to achieve compliance, helping you to identify suitable evidence along the way to support your claim of compliance.

Our findings are presented in an easily understood format that your team can easily understand, aiding teamwork and helping you to make timely, fact-based decisions that you can be confident of.

If you need to acquire additional technology, our Information Assurance and Cyber Security consultants are also on hand to help you choose the most suitable products and services to help you along your journey.

From the simplest contracts to the most complex, Thales has the skills and experience that you need to achieve compliance faster and more easily.


facebook.com/thalesgroup


twitter.com/thalesgroup


linkedin.com/company/thales


youtube.com/thethalesgroup

THALES

350 Longwater Avenue
Green Park, Reading
RG2 6GF, United Kingdom
Email: thalescyberandconsulting@uk.thalesgroup.com
www.thalesgroup.com/en/tcc-uk