Supplier – Frequently Asked Questions

Content

What is the Cyber Threat?

The cyber threat refers to economic and industrial espionage perpetrated against Government and industry through attacks against IT infrastructure. Espionage of this type is a threat to any organisation whose livelihood depends on information.

The attackers of most concern are nation states, organised crime and hackers looking to gain economic, military or strategic advantage. They are highly motivated and capable and the consequences to an organisation of being compromised could be serious, resulting in financial loss, reputational damage and a reduction in share price / shareholder confidence. The information targeted can include intellectual property, operational information as well as commercially sensitive information such as pricing.

In an increasingly interconnected world, cyber threats can only be combatted through a coordinated approach across Governments and Industry including the defence primes and the supply chain. This approach is founded on building awareness, sharing threat intelligence and collaborating on cyber security strategies and approaches.

Back to Top

What are the benefits to my company in completing the cyber security questionnaire?

We suggest that the questionnaire should take no longer than 1 hour to complete assuming that it is completed with input from the function in your organisation responsible for Information / IT Security or IT (where a specific security function does not exist).

For organisations who are less aware of the cyber threat, participating in the questionnaire can act as the first step in raising awareness of cyber security in your organisation. BAE Systems can share guidance and other materials (inc. a training course) that can help your organisation better understand cyber risk and in time improve management of the risk.

For organisations that are aware of the cyber threat, participating in the questionnaire will enable you to demonstrate the effectiveness of your organisational cyber security capabilities. Increased cyber security maturity directly correlates with an ability to secure sensitive information, engenders confidence, and creates competitive advantage. BAE Systems can share guidance and other materials (inc. a training course) that may be of some assistance to your cyber security programme.

BAE Systems is currently in consultation with other Defence Primes and industry groups about how to address Cyber risk in the aerospace and defence supply base as cost effectively as possible. One opportunity under consideration is sharing answers to the Supplier Questionnaire between Defence Primes to reduce the need for suppliers to complete multiple questionnaires. At this point in time, supplier information will not be shared outside BAE Systems. Should BAE Systems decide to participate in a data sharing scheme in future, supplier information will not be shared unless the supplier has been consulted and has given their authorisation.

Back to Top

Why is my company being asked to fill out the cyber security questionnaire?

BAE Systems relies on suppliers to be successful in delivering products and services to customers. Cyber Security threats are real and a reliable avenue to compromise sensitive information. Companies across the aerospace and defence sector are being targeted for the sensitive intellectual capital they possess.

Defence primes have long recognised the cyber threat and the damage it can cause to individual organisations and economies as a whole. Increasing numbers of security incidents and requirements from Government customers are driving initiatives to improve cyber security defences in the supply chain.

As Prime contractors have enhanced their cyber security defences, threats have expanded across the entire supply base. Suppliers vary in their capabilities to address these threats and protect sensitive programme information.

It is imperative to engage proactively with suppliers to better understand their level of cyber security maturity, build awareness, and reduce risk. This engagement is designed to help suppliers mature in cyber security. It is also to help programme and capture team members understand how to better manage programme risk and lower costs.

The cyber security questionnaire specifically relates to leading indicators of cyber security maturity. The Supplier Cyber Security indicators will be one criteria in guiding companies to manage overall risk. It will be an indicator of a supplier's cyber security maturity or highlight the need to mitigate risks of sharing sensitive information with them if they are less mature.

Back to Top

Will filling out the cyber security questionnaire make me a preferred supplier?

The cyber security questionnaire provides one input to manage risk. A supplier's increased cyber security maturity directly correlates with its ability to secure sensitive information, engenders confidence, and creates competitive advantage. Those suppliers with a lower cyber security maturity, raise questions, require more risk mitigation, and possibly drive increased costs.

Back to Top

How will my answers to the Cyber Security questionnaire be used?

The answers to the cyber security questionnaire provide leading indicators of cyber security maturity. The Supplier Cyber Security indicators are one criterion in guiding companies to manage overall risk. It is an indicator of a supplier's cyber security maturity or highlights the need to mitigate risks of sharing sensitive information with them if they are less mature.

Back to Top

Who will have access to my information that is submitted to BAE Systems?

BAE Systems treats all information collected from suppliers throughout the Supplier Cyber Security Process in Strict Confidence and secures it accordingly. Access to this information is managed on a "least privilege model". Only those individuals within BAE Systems that have a need to know the information to perform their role will have access. All information is stored in our access controlled document management system on our secure networks.

BAE Systems will not share any information with third parties. Should a requirement arise in the future to share information with another organisation, information will not be shared unless the supplier has been consulted and has given their prior authorisation.

Back to Top

If I make investments to improve my cyber security maturity what will happen?

A supplier that focuses resources on improving its cyber security maturity can be better prepared to meet cyber security threats. A supplier's increased cyber security maturity directly correlates with its ability to secure sensitive information, engenders confidence, and can create competitive advantage.

Back to Top

Do you have any recommendations for an approved system?

The desire is that companies have the ability to secure sensitive information. Securing sensitive information and systems are dependent upon several criteria. As a first step, it is suggested that suppliers review the topic areas covered in the cyber security questionnaire and determine the best way to implement them.

Back to Top

How does this survey affect contracts?

This survey does not affect contracts. It does not constitute a change to any contracts and shall not serve as the basis for any claim against contracts. Completing the survey does not relieve your company from compliance with any term of contracts.

Back to Top

Will money be provided to suppliers to pay for cyber security protection improvements?

No. Cyber-security protections are not chargeable to contracts.

Back to Top

How often do we have to complete the questionnaire?

In future, we intend that suppliers will be able to provide updates to the Supplier Questionnaire at any time ensuring that we have the most up to date information about your organisation. As a minimum we intend that suppliers should review their answers to the Supplier Questionnaire as part of BAE Systems supplier assurance process.

Back to Top

Can we have additional information / guidance on specific cyber-security questions?

There are many resources that can help a supplier set up a cyber-security programme. Some useful resources can be found in the table below:

SANS (SysAdmin, Audit, Network, Security) Institute	www.SANS.org
Open Web Application Security Project (OWASP)	www.owasp.org
National Institute of Standards and Technology – Computer Security Division	http://csrc.nist.gov/
International Organization for Standardization	http://www.iso.org/iso/ (search ISO 27001 and 27002)
Cyber-security Information Sharing Partnership (CISP)	www.cisp.org.uk

Back to Top