Supplier Cybersecurity Questionnaire
FREQUENTLY ASKED QUESTIONS

Q1. Why is my company being asked to fill out the Cybersecurity Questionnaire?

As a valued or prospective supplier to BAE Systems, Boeing, Lockheed Martin, Raytheon and/or Rolls Royce (herein referred to as "the Exostar partners"), you play an important role in protecting our networks and the information you access from those networks from cyber threats. Cybersecurity threats are real and reliable avenue to compromise sensitive information. Companies are being targeted for the sensitive intellectual capital they possess. The questionnaire helps us better understand your cybersecurity posture and manage risks associated with sharing our sensitive information with your company.

We are all interconnected and as such a risk in one company affects all the partners. No one is immune from cyber-attacks and as such, it essential that we understand the capabilities you have in place to guard against the cyber threat so that we can mitigate risks where appropriate.

The cybersecurity questionnaire provides leading indicators of a supplier's cybersecurity maturity. It is an indicator of a supplier's ability to protect sensitive information shared with the supplier. A supplier's answers are one criterion in guiding companies to manage overall risk and continue to be successful in the critical business they do.

Q2. What is the Cybersecurity Questionnaire?

The Cybersecurity Questionnaire is a self-administered assessment tool designed to provide leading indicators of respondent's cybersecurity capabilities. It is derived from industry best practices and largely based on the recommended cybersecurity controls as prescribed by the Council on Cybersecurity (formerly known as the SANS Top 20). This questionnaire will be revised in the future based on evolving threats and industry best practices. Every effort will be made to balance the need to update the questionnaire and minimize the burden on respondents. When accurately completed, the results of the questionnaire will provide guidance on your present cyber protection capabilities and how you may improve your security posture. The controls contained within the questionnaire should not be seen as the only controls needed but serve as a guide of where to start.

Q3. How are the Cybersecurity Questionnaire results used by the Exostar partners?

The answers to the Cybersecurity Questionnaire provide leading indicators of cybersecurity maturity. The Supplier Cybersecurity indicators are one criterion in guiding companies to manage overall risk. It is an indicator of a supplier's ability to protect sensitive information. Each of the Exostar partners may use the results to make individual business risk decisions based upon your responses and the resulting capability level. Therefore, it is imperative that the questionnaire be completed accurately by the appropriate qualified personnel. Suppliers are encouraged to keep the Cybersecurity Questionnaire accurate and as up to date as possible as enhancements to your cybersecurity controls are made to most accurately reflect your cybersecurity posture.

Supplier Cybersecurity Questionnaire
FREQUENTLY ASKED QUESTIONS

Q4. What does cybersecurity capability mean?

It is an indicator of a supplier's ability to guard against cyber-attack. A higher cybersecurity capability directly correlates with the ability to protect sensitive information. It potentially engenders confidence and may create competitive advantage. In contrast, a lower cybersecurity capability could raise questions regarding a supplier's ability to adequately protect sensitive information and may require more risk mitigations. Cybersecurity Capability levels range from Level 0 through Level 5 and are defined as follows:

Level 0	Indicates no or minimal cyber risk management program; significant cyber protections are lacking; additional risk mitigations must be implemented
Level 1	Indicates a basic level cyber risk management program; some protections in place but additional risk mitigations must be implemented
Level 2	Indicates a moderate level cyber risk management program; good protections in place but additional risk mitigations are required to protect sensitive information
Level 3	Indicates a solid performing cyber risk management program; strong protections have been implemented; Advanced threats are understood and taking steps to address with specific controls; Additional risk mitigations are likely needed to protect against advanced attacks
Level 4	Indicates a cyber risk management program that can detect, protect against, and respond to advanced threats; Specific advanced controls are implemented
Level 5	Indicates a cyber risk management program that can detect, protect against, and respond to advanced threats; Specific advanced controls are implemented and optimized on an ongoing basis

Q5. How should I go about completing the questionnaire?

Once you have received your invitation to complete the questionnaire, it is recommended you meet with your IT security team and/or IT staff to gather the necessary information and then input your company's responses into the Exostar Partner Information Manager system.

In addition, the Critical Security Controls document should be used as a guide to help you understand the specific security control objective and respond accordingly to the corresponding control questions.

For BAE Systems, Boeing, Raytheon, and Rolls Royce suppliers:

- Go to https://portal.exostar.com and login or follow the instructions in the First Time Login email you received from Exostar to establish your account.
- Click the "Open Application" link for Partner Information Manager. If you are the first PIM user in your organization, you will need to accept the Service agreement by clicking the "View Service Agreement" link.
- If you have a pending Relationship with a PIM Subscriber Organization, please action by clicking the PENDING link in the "Buyers" gadget or the button in the red notification in the right sidebar.
- Click "Respond" on the Cybersecurity Questionnaire in the "Questionnaires to Complete" section.

Lockheed Martin Suppliers:

- Go to https://portal.exostar.com and login
- Click on the "My Account" tab
- Click on "View Organization Details"

- Click on "View in Trading Partner Manager (TPM)"
- (Must have Organization Administrator rights to access TPM; to see who has those rights please see the "Organization Administrator" section of the "View Organization Details" page)
- Click "Continue" if prompted
- Click on "Self-Certification" on the left side menu

Q6. I have completed the questionnaire, now what?

Upon completion of the questionnaire, an overall capability level will be generated based upon the responses. We will use the results to understand your ability to guard against cyber-attack and assess the risk of sharing sensitive information with your company. Suppliers are encouraged to use the results to identify areas to improve their security posture and manage their cyber risk.

All suppliers with whom sensitive information is being shared should meet a minimum capability of Level 3 to demonstrate a solid cybersecurity risk management program. It is recognized that all suppliers will not be able to immediately attain capability level 3. Please understand that this is the baseline set of controls for a solid cybersecurity risk management program and while the controls outlined will not block a supplier from all attacks it will get a supplier to a position where they are actively managing risk. This is the main goal, for suppliers to be active partners in managing cyber risk and protecting sensitive information. It is ultimately up to each supplier to determine where their focus should be based upon their availability of resources as well as constraints.

Q7. How does this questionnaire differ from DFARS 252.204-7012?

DFARS 252.204-7012 outlines a specific set of controls required to protect a certain type of data for a specific customer. The Cybersecurity Questionnaire is designed to highlight and ask about a set of controls that will help protect information and infrastructure regardless of the customer. While this questionnaire supports DFARS, it is only intended to provide leading indicators of a supplier's cybersecurity capability. It DOES NOT check for DFARS compliance. If a supplier's results reflect a low capability level, they may not do well in complying with DFARS controls. If a supplier rates well, then it is likely they may do better in complying with DFARS compliance.

NOTE: The DFARS contract clause and associated NIST controls specifically outline cyber requirements to protect Controlled Unclassified Information (CUI). It is suggested that the Cybersecurity Questionnaire and rating be used to give leading indicators of a supplier's ability to protect sensitive information and CUI. A supplier must do a complete analysis of their DFARS compliance if they have Controlled Unclassified Information (CUI). Completion of this questionnaire and any ratings developed as a result are not to be considered evidence or validation that the supplier meets the requirements of DFARS 252.204-7012.

Q8. Will filling out the Cybersecurity Questionnaire make me a preferred supplier?

No, the Cybersecurity Questionnaire provides one input to manage risk. A supplier's increased cybersecurity maturity directly correlates with its ability to secure sensitive information, engenders confidence, and can create competitive advantage. Those suppliers with a lower cybersecurity maturity, raise questions, require more risk mitigation, and possibly drive increased costs.

Supplier Cybersecurity Questionnaire
FREQUENTLY ASKED QUESTIONS

Q9. How often will the questionnaire change?

This questionnaire will be revised in the future based on evolving threats and industry best practices. Every effort will be made to balance the need to update the questionnaire and minimize the burden on respondents.

Q10. What is the scope of the Cybersecurity Questionnaire?

The scope of the questionnaire includes all aspects of your organization's information security program and technology infrastructure. Any cybersecurity compromise of a company can lead to additional compromises, impaired ability to perform contract deliverables, and loss of data in other areas of the infrastructure, including leveraging the infrastructure of a compromised supplier to attack a business partner or customer.

Q11. If I make investments to improve my cybersecurity capability what will happen?

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

Q12. 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.

Q13. Will money be provided to the supplier to pay for cybersecurity protection improvements?

No, cybersecurity protections are not chargeable to contracts. Implementing appropriate cybersecurity controls within a company's IT infrastructure is considered a necessary element of routine business practices and aligns with industry expectations.

Q14. Can we have additional information and guidance on the specific cybersecurity questions?

There are many resources that can help a supplier establish a cybersecurity risk management program. Some useful resources are found below:

- Center for Internet Security: http://cisecurity.org/
- Council on Cybersecurity - https://www.cisecurity.org/controls
- National Institute of Standards and Technology – Computer Security Division - http://csrc.nist.gov/
- Other resources that may be useful are:
  - International Organization for Standardization - https://www.iso.org/standards.html search ISO 27001 and 27002
  - Open Web Application Security Project (OWASP) - www.owasp.org