

**DFARS 252.204-7012 Compliance Assertion Report**

Contract : SALIMA0786756

Organization Name : United Tech Inc.

Exostar ID : 119963394

Exported By : Salima Washington

Export Date : 12/05/2018 09:34 AM

**Background**

As an identified subcontractor to Contract : SALIMA0786756, your organization was requested to complete the DFARS 252.201-7012 Compliance Assertion Form. The questions in this form concern your obligations under DFARS 252.204-7012, Safeguarding Covered Defense Information(CDI) and Cyber Incident Reporting(OCT 2016).

Within this form, you have answered the following for the questions listed below (as stated in this DFARS 252.201-7012 form) in the Questions and Responses section of this report.

**Questions & Responses**

Question	Yes	No
1. Does your organization receive or generate CDI in the performance of the referenced DoD contract?		
11. Has your direct customer for this contract flowed down to your organization the requirements of DFARS 252.204-7012?		
12. Have you implemented the security controls required in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171r1, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations? (ref: <a href="https://www.nist.gov/node/1130741">https://www.nist.gov/node/1130741</a> )		
121. Have you documented how you implement those controls in your required System Security Plan (SSP)? You may be required to provide validation as part of an RFP response, during the damage assessment process after a breach, or a compliance audit.		
122. Are any unimplemented or deficient controls documented in a Plan of Action and Milestones (POAM)? You may be required to provide validation as part of an RFP response, during the damage assessment process after a breach, or a compliance audit.		
13. Do you have a DoD-approved medium assurance certificate to “rapidly report” cyber incidents to the DoD CIO within 72 hours to <a href="https://dibnet.dod.mil">https://dibnet.dod.mil</a> ?		
14. Do you have any suppliers who receive or generate CDI in their performance of their DoD subcontracts for the referenced contract?		
15. Is any of the CUI generated, stored or processed by your organization stored in an IT system directly accessible to the Internet (see guidance information)?		
16. Does your organization enforce a policy that prevents the use of personal devices (example: BYOD policy is not allowed)?		
17. Does your organization utilize e-mail filtering to identify malicious links, attachments, etc.?		
18. Does your organization use an internet proxy capability to block/manage employee web browsing access to the Internet (example: block access to "uncategorized" websites)?		
19. Does your organization regularly scan and remediate issues identified on your perimeter systems (example: regular patching, retire end-of-life systems)?		

**List of Suppliers**

If you answered "yes" to question 14 above, below are the list of your suppliers (and the requested supporting details) who you stated as those who receive or generate CDI in the performance of their DoD subcontracts for thereferenced contract.

Supplier Name :	
Business Unit :	Contact Name :
DUNS Number :	Contact Email Address :
Address :	DFARS 252.204-7012 clause for CUI was flowed down to this supplier :
City :	MDA supply chain pilot contractual requirements flowed down to this supplier :
State :	
Postal Code :	
Country :	
Telephone Number :	

**Form Contact information**

Listed below is the contact information supplied for the answers provided in this form.

Contact Name :
Email Address :
Title :