

SUPPLY CHAIN ASSESSMENT (SOFTWARE)

SUPPLIER INFORMATION

Company Name:		
Address:		
City:	State:	Country (if outside USA):
Name & Title of person completing this assessment:		
Phone:	Email:	

BUSINESS INFORMATION

Primary Product(s)/Services(s):		
Are there multiple business locations? <input type="checkbox"/> Yes <input type="checkbox"/> No		
If yes, please indicate the following: <input type="checkbox"/> same as above		
Headquarters Name:		
Headquarters City:	State:	Country:

QUALITY, SECURITY, & COMPLIANCE REGISTRATIONS/CERTIFICATIONS

<ul style="list-style-type: none"> Attach a current copy of the certificate for each registered standard For policies not registered/certified, attach documentation supporting compliance (e.g., policy, quality manual, etc.) 		
<input type="checkbox"/> ISO/IEC 27001:2013	<input type="checkbox"/> Registered	<input type="checkbox"/> Compliant
<input type="checkbox"/> ISO9001-2015	<input type="checkbox"/> Registered	<input type="checkbox"/> Compliant
<input type="checkbox"/> Other (CMMI, SOC, SSAE) please list below:		
<input type="checkbox"/> Other (please list):	<input type="checkbox"/> Registered	<input type="checkbox"/> Compliant
<input type="checkbox"/> Other (please list):	<input type="checkbox"/> Registered	<input type="checkbox"/> Compliant
<input type="checkbox"/> We have Quality Assurance policies that are not affiliated with specific recognized standards.		
<input type="checkbox"/> We currently do not have any Quality Assurance policies, but will establish quality policies to meet this requirement if awarded a subcontract. (Suggested assistance and templates are available at https://www.nmptac.org/ or https://www.nmptac.org/resources/)		

Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	1. Does your organization have a documented process for gathering requirements? (e.g., customer-provided, system, program, product, etc.) If No or N/A , please explain:
Yes <input type="checkbox"/> No <input type="checkbox"/>	2. Does your organization employ static testing methods on all products/deliverables? <i>Distributors: Can you supply documentation from the manufacturer/developer demonstrating or supporting the use of static testing on deliverables?</i> (a) If yes, please attach. (b) If no, please explain:
	3. Does your organization (or the product developer) analyze all compiled code to identify and verify: (a) All Third-Party Software (TPS) and/or Open Source Software (OSS) components <input type="checkbox"/> Yes <input type="checkbox"/> No (b) Review components against all known vulnerabilities found in the National Vulnerability Database (nvd.nist.gov) or similar vulnerability list such as Common Vulnerabilities and Exposures (CVE) Open Web Application Security Project (OWASP), etc.? <input type="checkbox"/> Yes <input type="checkbox"/> No If No , how does your organization (or the developer) assure the quality and security of deliverables, including applicable Third-Party Software (TPS) and/or Open Source Software (OSS)?

SUPPLY CHAIN ASSESSMENT (SOFTWARE)

Yes <input type="checkbox"/> No <input type="checkbox"/>	4. Does your organization (or the product developer) analyze product behavior during operation and whether such behavior introduces potential security vulnerabilities that could negatively impact confidentiality, integrity, and availability? If No , please explain:
N/A <input type="checkbox"/>	5. Please describe your product license management model: (e.g., are licenses delivered or renewed automatically from a cloud?) Description of license management model:
Yes <input type="checkbox"/> No <input type="checkbox"/>	6. Will the proposed product or deliverable have remote system maintenance capabilities, software upgrades, troubleshooting, and diagnostics? If yes , does the remote mechanism: (a) utilize strong authentication for access to products? <input type="checkbox"/> Yes <input type="checkbox"/> No (b) assure the download packages are unaltered, malware-free and from a trustworthy supplier? <input type="checkbox"/> Yes <input type="checkbox"/> No
Yes <input type="checkbox"/> No <input type="checkbox"/>	7. Does your organization have a documented policy or procedure for protecting electronic data and systems from unauthorized viewing/use? If No , please explain:
Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	8. Is physical access to your facility and/or systems monitored and logged? Are access records maintained? If No or N/A , please explain:
Yes <input type="checkbox"/> No <input type="checkbox"/>	9. Does your organization subscribe to and maintain antivirus product on all employee workstations? What products are used? If No , please explain:
Yes <input type="checkbox"/> No <input type="checkbox"/>	10. Have you ever experienced a significant cybersecurity incident or data breach? If Yes , please define the incident and describe remediation actions:
Yes <input type="checkbox"/> No <input type="checkbox"/>	11. Is your company International Traffic in Arms Regulations (ITAR) registered? If No , do you have procedures to handle ITAR requirements? <input type="checkbox"/> Yes <input type="checkbox"/> No
Yes <input type="checkbox"/> No <input type="checkbox"/>	12. Are you willing to provide product documentation disclosing features and functions of deliverables? (a) If Yes , please attach. (b) If No , please explain:

Date

Signature (person completing assessment)

This report may be shared with the Dept. of Energy (DOE), National Nuclear Security Administration (NNSA), and with other DOE/NNSA operating subcontractors.

For NTESS/Sandia Internal Use Only		
Reviewed by: _____	Organization: _____	Date: _____
Status		
Approved: <input type="checkbox"/>	Conditional: <input type="checkbox"/>	Not Approved: <input type="checkbox"/>