Sandia National Laboratories

# 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? ☐Yes ☐No | | |
| If yes, please indicate the following: ☐same as above | | |
| Headquarters Name: | | |
| Headquarters City: | State: | Country: |

**QUALITY, SECURITY, & COMPLIANCE REGISTRATIONS/CERTIFICATIONS**

- *Attach a current copy of the certificate for each registered standard*
- If compliance is indicated (without registration), attach documentation supporting compliance (e.g., policy, quality manual, etc.)

| | | |
|---|---|---|
| ☐ **ISO/IEC 27001:2013** | ☐ Registered | ☐ Compliant |
| ☐ **ISO9001-2015** | ☐ Registered | ☐ Compliant |
| ☐ **Other (CMMI, SOC, SSAE) please list below:** | | |
| ☐ **Other (please list):** | ☐ Registered | ☐ Compliant |
| ☐ **Other (please list):** | ☐ Registered | ☐ Compliant |
| ☐ **Other (please list):** | ☐ Registered | ☐ Compliant |

| | |
|---|---|
| Yes☐ No☐ N/A☐ | 1. Does your organization have a documented process for gathering requirements? (e.g., customer-provided, system, program, product, etc.)<br><br>If **No or N/A**, please explain: |
| Yes☐ No☐ | 2. Does your organization employ static testing methods on all products/deliverables?<br><br>*Distributors: Can you supply documentation from the manufacturer/developer demonstrating or supporting the use of static testing on deliverables?*<br><br>(a) If yes, please attach.<br><br>(b) If no, please explain: |
| | 3. Does your organization (or the product developer) analyze all compiled code to identify and verify:<br><br>(a) All Third-Party Software (TPS) and/or Open Source Software (OSS) components<br>☐Yes ☐No<br><br>(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.?<br>☐Yes ☐No<br><br>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☐ No☐ | 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?<br><br>If **No**, please explain: |
| N/A☐ | 5. Please describe your product license management model: (e.g., are licenses delivered or renewed automatically from a cloud?)<br><br>**Description** of license management model: |
| Yes☐ No☐ | 6. Will the proposed product or deliverable have remote system maintenance capabilities, software upgrades, troubleshooting, and diagnostics?<br><br>**If yes**, does the remote mechanism:<br>(a) utilize strong authentication for access to products?<br>☐Yes ☐No<br><br>(b) assure the download packages are unaltered, malware-free and from a trustworthy supplier?<br>☐Yes ☐No |
| Yes☐ No☐ | 7. Does your organization have a documented policy or procedure for protecting electronic data and systems from unauthorized viewing/use?<br><br>If **No**, please explain: |
| Yes☐ No☐ N/A☐ | 8. Is physical access to your facility and/or systems monitored and logged? Are access records maintained?<br><br>If **No or N/A**, please explain: |
| Yes☐ No☐ | 9. Does your organization subscribe to and maintain antivirus product on all employee workstations? What products are used?<br><br>If **No**, please explain: |
| Yes☐ No☐ | 10. Have you ever experienced a significant cybersecurity incident or data breach?<br><br>If **Yes**, please define the incident and describe remediation actions: |
| Yes☐ No☐ | 11. Is your company International Traffic in Arms Regulations (ITAR) registered?<br><br>If **No**, do you have procedures to handle ITAR requirements? ☐Yes ☐ No |
| Yes☐ No☐ | 12. Are you willing to provide product documentation disclosing features and functions of deliverables?<br><br>(a) If **Yes**, please attach.<br><br>(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: ☐ | Conditional: ☐ | Not Approved: ☐ |