|  |
| --- |
| **Supply Chain Risk Management Checklist** |
| Program Name: U.S. Department of State Evolve IDIQ |
| Date of Assessment: |
| Name of Assessor: |

|  |  |  |  |
| --- | --- | --- | --- |
| **Acquistion** | | **Yes** | **No** |
| 0 | Have you identified your key suppliers? |  |  |
| 1 | For all suppliers, do you verify company ownership? Confirm U.S. ownership? |  |  |
| 2 | Do you verify country of origin for all supplies, down to the very first source? |  |  |
| 3 | If you use distributors, do you investigate them for potential threats? |  |  |
| 4 | Can you provide a list of companies from whom your firm purchases all COTS software? |  |  |
| 5 | Do you safeguard key program information that may be exposed through interactions with subs and suppliers? |  |  |
| 6 | Do you perform reviews, inspections, and have safeguards to detect/avoid counterfeit |  |  |
| 7 | Do you use the NES (Network Security) baseline when purchasing software? |  |  |
| 8 | Do you comply with ITAR rules? |  |  |
| 9 | Do you have procedures for securely upgrading software in the field? |  |  |
| **Design/Development** | |  |  |
| 11 | Will the companies currently performing engineering for your firm support your firm during performance on Evolve? |  |  |
| 12 | Do only U.S. citizens have access to your design network? |  |  |
| 13 | Are you aware of who will develop your training and technical manuals? |  |  |
| 14 | Are you using trusted software development tools? |  |  |
| 15 | Are you using trusted information assurance controls to safeguard technical data in the development environment (networks, PC’s test equipment and configuration systems)? |  |  |
| 16 | Does your firm evaluate open-source software? |  |  |
| 17 | Are your software compilers controlled for authorized access only? |  |  |
| 18 | Do you know how your supplier will test and configure software code? |  |  |
| **Logistics** | |  |  |
| 19 | Does your program have documented configuration management, tracking and version control? |  |  |
| 20 | Have you thought about what events (environmental or man-made) can interrupt your supply chain? |  |  |
| 21 | Do you have a process that ensures integrity when ordering inventory? |  |  |
| 22 | Are upgrades to your IT infrastructure evaluated for possible tampering? |  |  |
| 23 | Is there a documented chain of custody for the deployment of products and systems? |  |  |
| **Policy and Procedures** | |  |  |
| 24 | Do you have definitive policies and procedures that help minimize supply chain risk? |  |  |
| 25 | Do you define and manage system criticality and capability? |  |  |
| 26 | Does everyone associated with the program (program managers, prime contractors, subcontractors, etc.) understand the threats and risks in the program’s supply chain? |  |  |
| 27 | Do you have "insider threat" controls in place? |  |  |
| 28 | Do you use any protective technologies? |  |  |
| 29 | Do you use, record, and track risk mitigation options throughout project or purchase lifecycle? |  |  |
| 30 | Have all of your contractors signed non-disclosure agreements? |  |  |
| 31 | Do you make your supply chain risk management policies/procedures a requirement for all subcontractors, teaming partners, suppliers, etc.? |  |  |
| 32 | Do your supply chain risk management policies/procedures take into account secondary risks? |  |  |
| 33 | Do you develop and use a Risk Management plan? |  |  |
| 34 | Does anyone have access to your data from an external connection? |  |  |
| 35 | For contractors who use your data on their system, do they have adequate security controls? |  |  |

1. For Items Answered “yes” above, provide a description of “how” the firm conducts each process (and what tools are used, if applicable).
2. Describe Why You answered No for Any of the Above: