Attachment J-11
Cybersecurity and Supply Chain Risk Management (SCRM) Assessment Template

This attachment is in support of solicitation 47QTCB20R0005.
Refer to Section L, Paragraph L.16 of the solicitation for further information.

The following outline and example content is not intended to be exhaustive or complete, but rather to serve as a starting point for your submission. There may be information and/or scenarios not covered in the examples which need to be addressed. Adapt and add details as you deem appropriate. The amount of space allocated in this outline does not indicate a limit on the content you can provide. Use an Arial font, no smaller than 10 point for your submission. The completed submission may not exceed a total of seven pages. Text exceeding seven pages will not be considered. You may edit and submit this template or create a completely new document.

Part A: Corporate identity and known/proposed relationships

1. Outline the offeror's corporate identity, including all parent and/or subsidiary entities.

Example 1:
We are company ABC, Inc, incorporated in the state of Maryland. Our DUNS number is 123456789. Our SAM.gov and Dynamic Small Business Search records provide a detailed profile of our firm. We do not have a parent organization or any subsidiaries.

Example 2:
We are company ABC, Inc, incorporated in the state of Maryland. Our DUNS number is 123456789. Our SAM.gov and Dynamic Small Business Search records provide a detailed profile of our firm. While we do not have a parent organization or any subsidiaries, we are offering as a SBA 8(a) mentor-protege JV. Our team brings together a newer 8(a) and an 8(a) STARS II alumnus as a mentor, CDE LLC., whose DUNS number is 987654321 and whose SAM.gov record provides a detailed profile of it.

Example 3:
We are company ABC, Inc, incorporated in the state of Maryland. As an Alaska Native Corporation, we do have a parent organization. Our DUNS number is 123456789. Our SAM.gov and Dynamic Small Business Search records provide a detailed profile of our firm. Our parent organization is CDE Inc, whose DUNS number is 987654321 and whose SAM.gov record provides a detailed profile of it.

2. Identity DUNS and names of any known subcontractors, suppliers, distributors and original equipment manufacturers (OEMs) involved in the offeror's supply chain and outline activities taken to identify, manage and mitigate supply chain risk.

The known subcontractors, suppliers, distributors and OEMs involved in our supply chain include:

Example 1:
_____ DUNS _____. SAM.gov provides a detailed profile.

Example 2:
_____ DUNS _____. SAM.gov does not contain a detailed profile because it is focused on commercial business, however it is a publicly traded organization listed in the U.S. Security and Exchange Commission's (SEC) EDGAR system under the listed company name.

Part B: Status of SCRM and cybersecurity programs

1. **Discuss the status of the following programs and outline activities taken to identify, manage and mitigate supply chain and cybersecurity risk. Outline planned actions to establish programs which do not yet exist.**
    a. **Supply chain risk management program (NIST 800-161)**
    b. **Cybersecurity program (NIST 800-171)**

Example 1:
Each of the above programs are established and we have had no findings of material weaknesses or deficiencies in any program.

Example 2:
All of the above programs are established and we have no findings of material weaknesses or deficiencies in any program. To enhance our cyber security posture, we are planning to attain the following industry credential(s) within the next five years: _____ (list credential).

Example 3:
We have an established supply chain risk management program, but are still developing our cyber security program. Our JV partner, identified in Part A above, has an established program in that area, and holds the following relevant certification(s) _____.

2. **Outline your intention in regards to obtaining CMMC, the target certification level, and a tentative timetable for attaining it as well as any cybersecurity or SCRM-related industry certifications.**

Example 1:
We currently hold no cybersecurity or SCRM-related industry certifications but we do intend to obtain CMMC Level 1 certification by the end of 2022.

Example 2:
We have the following industry credential(s) _____ (list credential) and intend to obtain CMMC Level 3 certification within the next five years.

Part C: Facility locations

1. **Do you have procedures in place which will enable you to provide the name and location of facilities where known information systems, IT hardware and/or software to be provided under task orders will be designed, manufactured, packaged or stored prior to distribution.**

Example:
Yes, we only use original equipment manufacturers (OEMs) or vendor certified resellers for information systems and will require valid licenses for OEM equipment and/or software to be provided under task orders. These OEMs currently include: _____, all of which are listed above in response to Part A, 2.

Part D: Development and delivery

1. **Outline how the offeror will assure a separation of duties exists during the development process of any information system, IT hardware and/or software to be delivered under task orders.**

Example:
We use strict system security engineering processes in specifying and designing IT systems to protect them from internal and external threats as well as against hardware and software vulnerabilities. These procedures currently include: _____

2. **Outline the means and methods for delivering any information system, IT hardware and/or software that the offeror intends to provide under task orders. Specifically, the name(s) of known entities responsible for transport or storage. This information should also address whether known information systems, IT hardware and/or software will be direct-shipped to the requiring organization.**

Example:
We only use original equipment manufacturers (OEMs) or vendor certified resellers for information systems and ship all orders directly to the customer organization via _____ to mitigate risk.

3. **When information systems, IT hardware and/or software to be provided will include a service agreement, the offeror's plan to identify in task order proposals to the government the identity of the contractor/subcontractor(s) who will provide this follow-on service, and how the services will be delivered/deployed (e.g., via on-site service? Remotely via the internet?)**

Example:
We service all IT systems using our own employees and usually perform the work on site. If remote support is provided we mitigate cyber risk by _____.

4. **When contract performance will include disposal services of any information system, IT hardware and/or software required by the task orders, the offeror's plan to identify, in task order proposals to the government, the identity of the entities that will provide disposal services.**

Example:
We do not repair IT equipment. If non-functional equipment cannot be repaired by the OEM or an OEM-authorized vendor/trusted partner under product warranties and contractual obligations, it is destroyed by a certified data destruction provider.

5. **Outline how the offeror will maintain a high level of cybersecurity and SCRM readiness for performance of IT services to federal customers.**

Example:
We will maintain awareness through routine new-hire training as well as annual refresher training which includes _____. Additionally we conduct routine internal cybersecurity assessments.