**UNITED STATES SPECIAL OPERATIONS COMMAND**
7701 TAMPA POINT BOULEVARD
MACDILL AIR FORCE BASE, FLORIDA 33621-5323

SOAE DD MMM 2023

POLICY MEMORANDUM -23-11

MEMORANDUM FOR SPECIAL OPERATIONS FORCES ACQUISITIONS, TECHNOLOGY AND LOGISTICS - PROGRAM EXECUTIVE OFFICES AND DIRECTORATES

SUBJECT: Cybersecurity and Supply Chain Risk Management

1. **Purpose:** To provide direction on the inclusion of cybersecurity and supply chain security into any best-value/trade-off evaluation of an offeror's management plan.

2. **Background**: The emergence of China and Russia as challengers requires assurance that the USSOCOM industrial base is prepared to secure information and material from foreign influence or interdiction. Over the past twenty years, focused mainly on C-VEO, SOF AT&L's acquisition process has not required the same level of diligence required to support SOF campaigning in integrated deterrence. For many of our operational requirements, our contracting process must ensure that industry partners selected to support SOF have the management wherewithal to secure their cyber network and to control their supply chain and their sub-contractors.

3. **Actions**: In a best-value/trade-off solicitation, as part of the factor assessing the offeror's ability to manage the effort, program managers and contracting officers should consider the inclusion of the attached Sections L and M criteria (as amended based on the facts of the requirement) when appropriate to safeguard capabilities acquired for the unique USSOCOM mission. The program manager and contracting officer will also determine whether these criteria (or something similar) should be applied to any lowest-priced technically acceptable (LPTA) effort. The overall intent is to include the right language in Sections L&M that would allow the Government to evaluate a potential offeror higher or lower based on the risk its proposal poses to the SOF enterprise.

4. Any questions regarding this policy can be directed to Mrs. Jennifer Metty, Chief, Procurement Support Division, at (813) 539-0463, or jennifer.metty@socom.mil.

JAMES H. SMITH
Acquisition Executive

Attachment

## Examples - SECTION L

CYBER SECURITY

- L.X.X – The Offeror shall provide to the government, a system security plan and any associated plans of action developed to satisfy the adequate security requirements of DFARS 252.204-7012, and in accordance with NIST Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations” in effect at the time the solicitation is issued or as required by the contracting officer, to describe the contractor’s unclassified information system(s)/network(s) where covered defense information associated with the execution and performance of this contract is processed, stored, or transmitted. System Security Plan and Associated Plans of Action for a Contractor’s Internal Unclassified Information System *[Insert Contract Data Requirements List (CDRL)].*

- L.X.X – In order to be considered for award, the Offeror is required to implement NIST SP 800-171 in accordance with DFARS provision 252.204-7019. The Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see DFARS 252.204-7020) for each covered contractor information system that is relevant to its proposal. The Basic, Medium, and High NIST SP 800-171 DoD Assessments are described in the NIST SP 800-171 DoD Assessment Methodology located at https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171. The Offeror shall provide to the Government its Basic System Security Assessment and its assessments for each proposed subcontractor utilizing the DoD Assessment Methodology located at the OSD website provided above. The submitted basic assessments will be utilized by Government evaluation personnel to conduct medium or High NIST SP 800-171 DoD Assessments. The Offeror shall grant Government evaluation personnel all access required to conduct System Security Assessments in accordance with the NIST SP 800-171 DoD Assessment Methodology.

- L.X.X - The Offeror shall provide the government the system security plan(s) (or extracts thereof) and any associated plans of action for each of the Contractor’s tier one level subcontractor(s), vendor(s), and/or supplier(s), and the subcontractor’s tier one level subcontractor(s), vendor(s), and/or supplier(s), who process, store, or transmit covered defense information associated with the execution and performance of this contract. System Security Plan and Associated Plans of Action for a Contractor’s Internal Unclassified Information System *[Insert Contract Data Requirements List (CDRL].*

- L.X.X - The Offeror shall identify all covered defense information (CDI) associated with the execution and performance of this contract. In Volume X of the proposal, the Offeror shall include their CDI Protection Plan to include the actions necessary to identify and affirm marking requirements for all covered defense information, as prescribed by DoDM 5200.01 Vol 4, Controlled Unclassified

Information, and DoDI 5230.24, Distribution Statements on Technical Documents, to be provided to the Contractor, and/or to be developed by the contractor, associated with the execution and performance of this contract.

SUPPLY CHAIN RISK MANAGEMENT (SCRM)

- L.X.X – The Offeror shall provide the Government a Supply-Chain Risk Mitigation Plan in Volume X of their proposal. The Offeror's plan shall provide a thorough and complete analysis of the supply chain required and a detailed explanation that supports the intention to successfully perform the requirements of this contract. The Offeror's plan shall include a hierarchy of all components, supplies, materials, software, labor, etc. required to successfully perform the requirements of this contract. The Offeror's plan shall also include a graphical exhibit that accurately displays the supply-chain relationship of the prime offeror, all subcontractors, all suppliers to the prime and subcontractors, and any other companies that will be utilized to perform the requirements of this contract. The plan shall describe how the Offeror will identify and mitigate supply chain risks, to include the mitigation of potential supply or logistics disruptions, in the performance of this contract. "Supply chain risk" is defined as the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of any supplies, material, equipment or services necessary to successfully deliver or perform the requirements of this contract so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such supplies, services, equipment, or systems.

- L.X.X - The Contractor shall develop, deliver, and maintain the Program Protection Implementation Plan (PPIP) IAW the USG-provided Program Protection Plan (PPP) as posted to the bidder's library. *[Insert Contract Data Requirements List (CDRL].*

- L.X.X - The Contractor shall develop a SCRM Plan IAW the current version of CNSSD No. 505, section IV and National Institute of Standards and Technology (NIST) Special Publication 800-161, as revised to mitigate supply chain risk. The Contractor shall develop and implement a Counterfeit Parts Prevention Program in compliance with 48 CFR § 252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System, using SAE AS5553, SAE AS6171, SAE AS6081, IDEA-STD-1010B, or similar practices to prevent the inclusion of counterfeit parts or parts with malicious logic. The Contractor shall report any identified counterfeit parts via the GIDEP IAW 3.3.7.4. *[Insert Contract Data Requirements List (CDRL].*

**Examples - SECTION M**

CYBER SECURITY

- M.X.X –The extent to which the offeror details a disciplined, structured system security engineering (SSE) process and system security plan, including criticality analysis, in arriving at its system specification and design. Offerors who exhibit a more integrated, complete process and plan will receive a more favorable evaluation.

- M.X.X - Offerors that exhibit a more fully integrated plan (a plan that implements a greater number of safeguards up to a full-compliance score of 110), as described in the NIST SP 800-171 DoD Assessment Methodology, will potentially receive a more favorable evaluation. Offerors who exhibit a system security plan that lacks compliance with multiple elements of the NIST SP 800-171 standards, may receive a less favorable rating. Offerors whose system security plan assessments result in a score of 85 or below, may be assigned risk. No additional strengths will be awarded for an offeror's plan that exceeds the NIST SP 800-171 standards or the DoD Assessment Methodology.

SUPPLY CHAIN RISK MANAGEMENT

- M.X.X - The Offeror shall provide a thorough and complete analysis of the supply chain required and intended to perform the requirements of this contract. Offerors' plans that contain a complete analysis and description of their required supply-chain will potentially receive a more favorable rating. Offeror's plans that contain a complete hierarchy of all components, supplies, materials, software, and/or labor required to successfully perform the requirements of this contract may potentially receive a more favorable rating. Offerors' plans that contain a complete graphical exhibit that accurately displays the supply-chain relationships of the prime offeror, all subcontractors, all suppliers to the prime and subcontractors, and any other companies that will be necessary to perform the requirements of this contract, may potentially receive a more favorable rating. Offerors' plans that contain a comprehensive approach to the identification and mitigation of supply chain risks may potentially receive a more favorable rating. Offerors' plans that exhibit less-complete analysis, contain incomplete data, supply-chain gaps, or a greater number of uncertainties in their supply-chains, may be assigned risk. Offeror's plans that contain an incomplete hierarchy of all components, supplies, materials, software, and/or labor required to successfully perform the requirements of this contract may be assigned risk. Offerors' plans that are found to not contain an adequate approach or ability to identify and mitigate supply chain risks, to include the mitigation of supply or logistics disruptions, may be assigned risk.

- M.X.X –The extent to which supply chain risk protection, detection, and response procedures and activities are incorporated into the system acquisition and contract execution. Offerors whose procedures are more completely incorporated and results in

a greater level of supply-chain protection and risk mitigation, will receive a more favorable evaluation.

Note 1: KOs and PMs shall work with their Requiring Activity to understand and tailor the above section L&M examples their specific requirement to meet the intent of the Cyber Security and SCRM policy memorandum.
Note 2:  See technical/risk rating definitions in DOD Source Selection Guide.