REMARK Enterprise Cyber Flowdowns

Dated: December 19, 2024

1.0 Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

2.0 Protection of Data from Unauthorized Disclosure

The Seller shall protect unclassified DoD data from unauthorized access or disclosure in accordance with DoDI 8582.01 Security of Unclassified DoD Information on Non-DoD Information Systems, and the Program's Security Classification Guide (SCG).

If the Seller has access to CUI, the Seller will comply with the requirements set forth in DoDI 5200.48 where applicable to contractors, DFARS 252.204-7012, and will have a process to implement NIST 800-171 to safeguard CUI.

3.0 Seller Enterprise Cyber Security Requirements

3.1 Seller Enterprise Cyber Security Program

The Seller shall develop, implement, and maintain a Cyber Security (CS) program emphasizing protection of CUI as it resides on, or transits through, Seller owned or operated information systems. The Seller's CS practices shall adhere to applicable laws and regulations as defined in the Mandatory Clauses of Attachment D -FAR_DFARS. Seller Personnel performing functions with cyber responsibilities shall have a minimum level of cyber security training consistent with DoD 8140.01 and DoD 8570.01-M, where applicable.

3.2 Seller Cyber Security Management Plan

The Seller shall maintain the System Security Plan (SSP) IAW the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171r2.

Until such time that the Buyer flows down the appropriate DFARS provisions for the Notice of Cybersecurity Maturity Model Certification Level Requirements to the Seller and the Seller has achieved the contractually specified CMMC Level, the Seller shall make the following available to Government: SSP(s), and related documentation shall describe how the NIST SP 800-171 security requirements are implemented as required by DFARS 252.204.7012. The Seller shall fully cooperate in the Government's review of the SSPs at the Seller's facility on a non-interference basis. The Seller shall make its SSP available for Government review at the Seller's facility upon request from the Government. Seller may share SSPs directly with the Government and shall not be required to share copies of the SSPs with Buyer.

If the Government determines that the SSP does not adequately describe how the NIST SP 800-171 security requirements are implemented, then the Government shall notify the Seller of each identified deficiency. The Seller shall, where reasonably practical, correct any identified deficiencies within thirty (30) days of notification by the Government. Where correction within 30 days is not reasonably practical, the contracting officer may require the Seller to maintain a Plan of Action and Milestones (POAM) for the correction of the identified deficiencies. The Seller shall immediately notify the contracting officer of and failure or anticipated failure to mee a milestone in the POAM. Seller shall not be required to share any POAM with Buyer.

Upon conclusion of the correction period, the Government may conduct a follow-on review of the SSP at the Seller's facilities with 30 days' notice and mutually agreeable times and dates. The Government man continue to conduct follow-on reviews until the Government determines that the Seller has corrected all identified deficiencies in the SSP.

Until such time as the Seller achieves the contracted CMMC Level, the Government may, in its sole discretion or in response to a cyber incident, conduct subsequent reviews at the Seller's site to verify the information in the SSP. The Government may conduct reviews at any time upon thirty (30) days' notice to the Seller.

An Information System Continuous Monitoring Strategy (ISCM) that describes the system and includes continuous monitoring requirements, system architecture, and interfaces. The ISCM should also identify key personnel, continuous monitoring tools, supporting processes, communication plan, and the continuous improvement plan.

3.2.1 Seller's Computing Environment

The Seller shall provide the Buyer with a documented Cybersecurity Management Plan (CSMP) (**SDRL 069**) that summarizes the below information. In sections where there are concerns regarding proprietary data or other non-program specific corporate interests, summarized, and/or redacted information can be provided.

Detailed descriptions of the design and implementation of each system or subsystem(s) security requirements shall be provided.

Provide a description of the design and implementation of each security requirement. If a security requirement does not apply, or it is partially applicable to the proposed implementation, the CSMP shall include an explanation for that requirement.

The CSMP shall include the architectural diagrams, general descriptions of environments used to store CUI and a summary of the implementation of security functions; however, Seller shall not be required to provide any detail in architectural diagrams it believes will compromise the security of such systems.

3.2.1.1 Personnel

Responsibilities of Seller Cybersecurity Personnel relevant to the task shall be identified at a role level, including, where applicable, Information Security Advisors (ISAs), Asset Owners, System Administrators, Access Administrators, Information Authorities, Information Owners, Information Technology Infrastructure (ITI), support personnel and end-users or equivalent positions.

3.2.1.2 Systems and Subsystems

Detailed descriptions of the design and implementation of each system or subsystem(s) security requirements shall be provided. The Seller shall provide a Seller Environment Software Bill of Materials for each component and subcomponent in the CE IAW DI-PSSS-81656 and deliver IAW SDRL 281.

This shall flow down to all vendors and subcontractors:

- Summary technical descriptions of the implementation of security functions, performance, and constraints for the systems and subsystem(s)
- Provide justification, individually, of the compliance to, and adequacy of, the design and implementation for each security requirement. If a security requirement does not apply, or is partially applicable to the proposed implementation, the CSMP shall include an explanation for that requirement.
- Describe how the integrity of program information is preserved in environments with a network connected or unconnected state.

3.2.2 CS Risk Management

The CSMP shall include a definition of the overall security and risk control objectives that the program manages within the Seller's CE.

The CSMP shall address risks typically associated with facilities and how they are alleviated. Areas of risk to consider at a minimum:

- Inadvertent or malicious file corruption on the part of personnel.
- Inadvertent or malicious file corruption due to intrusions over a network.
- Theft or destruction of critical software or development tools.
- Loss of data/development equipment due to natural disasters.
- Administrative Information Assurance controls implemented for the program.
- Operational Information Assurance controls implemented for the program.
- Technical Information Assurance controls implemented for the program.

For each risk the Seller shall identify the following, at a minimum:

- Risk Identification: The Seller shall describe how risks are identified.
- Risk Ranking: The Seller shall describe how risks are ranked.
- Risk Mitigation:
    - The Seller shall describe how risks are mitigated.
    - Identify risks and rank them according to the consequences of leaving them unmitigated.
    - The Seller shall identify mitigation techniques already in place as well as unmitigated risks.

3.2.3 Compliance to NIST SP 800-171

The Seller shall attest that the Seller if fully or partially compliant with NIST SP 800-171 and NIST SP 800-172 upon request for Buyer's awareness only. A response of partial implementation shall not be grounds for Buyer to take any contractual action (including but not limited to termination, modification, or price reduction). The Seller shall attest that the following NIST SP 800-171 controls (where required by DFARS 252.204-7012) are addressed in any SSP and POAM as appropriate.

3.2.4 Foreign Disclosure - Information Systems

The CSMP shall disclose all locations Outside the Continental United States (OCONUS) that connect to the Seller's Information systems and have direct access to program information. The CSMP shall describe the process to mitigate risk associated with unauthorized access and foreign disclosure.

3.2.5 Foreign Disclosure – Supply Chain Risk Management

The CSMP shall describe the notification process of its logic bearing hardware, software, and firmware used by the Seller or its subcontractors (applicable components will be identified by Buyer) is owned by, operated by, supported by, or otherwise exposed to any person or entity which is not a U.S. Citizen or corporation, or which is owned or controlled by a person or corporation or other business entity which is not a U.S. citizen or business entity. "Controlled" means that the non-U.S. entity or person owns more than 50% of the entity.

The CSMP shall describe the notification process to the Government of any changes to the status of foreign ownership or control of the Seller or their subcontractors during the performance of the production SOW through the Government.

GE Aerospace (GE) requires suppliers to obtain approval before transmitting or displaying CUI to a foreign national individual or a foreign supplier. This approval must be obtained for each piece of CUI that will be shared by every supplier at all levels in the supply chain.

3.2.6 Annual Audits

The Seller shall obtain and maintain the contracted CMMC Level no later than one year after the CMMC rules go into effect and maintain this certification throughout the life of the contract. The Seller shall develop a CMMC Implementation Plan listing all controls implemented and planned for audit in their CMMC certification IAW DI-MGMT-82002 and deliver IAW SDRL 282. The Seller shall notify the PM Cyber Lead of the dates of any third party CMMC assessments NLT 60 days prior to the event. The Seller shall allow designated Government representatives to audit process. The Seller shall develop a Cybersecurity POAM listing all deficiencies from the CMMC audit IAW DI-MGMT-82190 and deliver IAW SDRL 283. This shall flow down to all subcontractors and vendors.