FRONTGRADE SUPPLY CHAIN

Supplier Cybersecurity Representation

2024

Frontgrade Technologies is committed to achieving the highest standards of ethics, integrity, and performance to provide the products and solutions necessary for our customers, and we expect the same from our suppliers and vendors. In the realm of Cybersecurity, Frontgrade suppliers and vendors must take care to safeguard and protect information from unauthorized access, destruction, use, modification, or disclosure. We expect suppliers and vendors to have risk-based Cybersecurity programs designed to mitigate emerging threats to their information systems, products, services, and supply chain and to comply with all applicable contractual and legal requirements.

In addition, Frontgrade's U.S. Government customers frequently include contract clauses that require contractors and subcontractors (at all tiers) to provide "adequate security" to safeguard certain types of government information on their internal systems, including the following FAR and DFARS contract clauses:

- FAR 52.204-21 – Requires supplier's compliance at time of award with a select subset of NIST SP 800-171 "basic safeguarding" Cybersecurity controls for internal systems with "federal contract information."
- DFARS 252.204-7012 – Requires supplier's implementation of NIST SP 800-171, prior to award, which includes Cybersecurity controls for internal systems with "covered defense information" (CDI). To have implemented NIST SP 800-171 for purposes of this DFARS clause, companies must have performed a self-assessment of their covered systems, completed a System Security Plan (SSP) and, as applicable, a Plan of Actions and Milestones (POAM) and obtained the DIBNET incident reporting medium level of assurance hardware certificate
- DFARS 252.204-7019 and DFARS 252.204-7020 – Requires implementation of NIST SP 800-171 in accordance with DFARS 252.204-7020 – Prior to award, suppliers must conduct a basic self-assessment of the 110 NIST 800-171 controls for each information system that will handle Covered Defense Information (CDI), and submit resulting scores and documentation to the Department of Defense (DoD) Website "Supplier Performance Rating System (SPRS).

To obtain additional information regarding the Cybersecurity controls visit please contact your Frontgrade representative.

Please provide your responses to the representations below and return a signed version to the cognizant Frontgrade Buyer or Subcontracts Administrator.

SUPPLIER REPRESENTATIONS

Suppliers should complete the questionnaire below by checking the YES/NO box and providing any comments/details as necessary.

For all information systems that will process Controlled Unclassified Information (CUI), Covered Defense Information (CDI), Control Technical Information (CTI), and/or non-public Federal Contract information (FCI) in the performance of an award resulting from this quote/proposal:

#	QUESTION	YES	NO
1	Are your company information systems compliant with the requirements of FAR 52.204-21 "Basic Safeguarding of Covered Contractor Information Systems"? [**Note**: To be compliant, the 17 NIST FAR controls have to be fully implemented. The requirements cannot be met with a Plan of Action and Milestone (POAM)]	□	□
2	Are these systems compliant with the requirements of DFARS 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting"?	□	□
2a	Has your company implemented all 110 controls of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 on your relevant information systems?	□	□
2b	If "No" to question 2a, is your company operating under a Plan of Action and Milestones (POAM)?	□	□

#	QUESTION	YES	NO
2c	If your company is operating under a POAM: (i) Please provide the POAM closure date: 3/31/25 (ii) Has your company implemented all 31 Basic Security Requirement controls of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171? (iii) Has your company implemented 100 or more controls of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171?	□ □	□ □
2d	Does your company currently hold a Medium Level of Assurance (MLOA) Certificate to access DIBNET portal for cyber incident reporting? If "Yes" to question 2d, please provide the name of the issuer: IDEN TRUST	□	□
3	Is your company compliant with the requirements of DFARS 252.204-7019 and DFARS 252.204-7020 "NIST SP 800-171 DoD Assessment Requirements"? Compliance requires the usage of the DoD Assessment Methodology, with submitted resulting scores to the Department of Defense website "Supplier Performance Rating System (SPRS). If "Yes" to question 3, please provide: i. Self-assessment or Defense Industrial Base Cyber Security Assessment Center (DIB CAC): Self ☒ DIB CAC □ ii. If Self-assessed, provide the date of the score submission to SPRS: 9/7/23 iii. If "DIB CAC", what level assessment? Medium □ High □ iv. DIB CAC assessment date:	□	□

Company Name:

Frontgrade Supplier Number:

Signature: ____

Printed Name:

Title:

Date: