10/21/2020

To: Vigor Suppliers

From: Director of Supply Chain Management

This message is to alert you of an upcoming requirement for certain Vigor suppliers to undergo a cybersecurity fitness assessment, recently mandated by the U.S. Department of Defense (DoD). The assessment must be completed by all suppliers who use their own IT systems to handle sensitive DoD information, e.g., suppliers who receive electronic files sent by Vigor containing sensitive design drawings or specifications. The basis for this requirement are new DFARS clause, DFARS 252.204-7019, Notice of NIST SP800-171 DoD Assessment Requirements, DFARS 252.204-7020, NIST SP800-171 Assessment Requirements, DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements.

To be clear, suppliers who do not handle sensitive DoD information are not required to complete the cybersecurity fitness assessment referenced above.

The type of sensitive DoD information this new requirement concerns is commonly referred to as "CUI" or "controlled unclassified information." CUI comes in various forms, including things such as drawings or specifications that bear an export-control marking (ITAR or EAR) or documents marked For Official Use Only (FOUO), etc.

As a practical matter, you can generally determine whether particular information is CUI by markings that indicate it is sensitive DoD information.

This new requirement becomes effective November 30, 2020. After that date, Vigor will be precluded, under any DoD prime contract containing DFAR 252.204-7019, DFAR 252.204-7020, and DFAR 252.204-7021, from issuing a PO to any supplier whose IT systems will handle CUI, unless and until the supplier has completed the necessary assessment. In that regard, suppliers who complete the assessment before November 30th will help themselves as well as Vigor and the U.S. Government.

To learn how you can complete an assessment for your company, visit: https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html. At that site, the publication *"NIST SP 800-171 DoD Assessment Methodology rev 1.2.1"* provides detailed instructions.

This new cybersecurity assessment requirement is part of the DoD's ongoing effort to secure the U.S. Defense Industrial Base sector against attacks from cyber criminals and enemy states. Your cooperation with this effort is both necessary and very much appreciated.

Thank you for your cooperation,

Guillermo Tapia
Director of Supply Chain Management
Vigor_Supply_Chain@Vigor.Net