CYBERSECURITY:

Cyberattacks targeting systems and data throughout the world is constantly increasing in both volume and sophistication. It is critical that our suppliers understand the risks associated with these attacks and implements appropriate security actions to successfully manage the Confidentiality, Integrity, and Availability of Govaged, Inc. sensitive data as well as DoD's Controlled Unclassified Information (CUI) as defined by DFARS Clause 252-204-7012.

Per DoD clause 252-204-7012, DoD contractors and subcontractors are required to implement and comply with security requirements to protect CUI data that is stored, processed, transmitted or used to generate data related to CUI as part of contract performance. These same requirements also apply to any Govaged, Inc. sensitive data provided to suppliers as part of DOD contract performance.

Please contact Govaged.Cyber@govaged.com for any cybersecurity questions.

USA: 4517 La Salle Ave, Alexandria VA 22304-1524
UK: 208 Pill Box Studios, 115 Coventry Road, London E2 6GG England
Ph.: 1.302.257.2327 | Fax: 1.302.450.1920
| Ph.: 1.302.608.0208
www.govaged.com | www.govaged.co.uk

CYBERSECURITY REQUIREMENT:

DFARS Clause 252-204-7012 defines the cybersecurity requirements to be complied with to manage Controlled Unclassified Information (CUI) as a DoD Contractor or Subcontractor. Some of the elements of this requirement include:

The use of NIST 800-171 as the security framework for protection of CUI. Contractors and Subcontractors need to be in compliance with the requirements in the DFAR clause as well as the NIST security framework by the end of December, 2017.

Areas of non-compliance will need to be reported to DoD within 30 days after contract award or within 30 days of any DoD related subcontract award from Govaged, Inc.

These requirements need to be flowed down to any subcontractors used in the performance of any DoD contract.

Any cyber incident (as defined by 252.204-7012) related to CUI data is to be reported to DoD via a reporting website within 72 hours of the incident discovery.

Govaged, Inc. suppliers are responsible to meet the requirements in DFAR 252-204-7012 and NIST 800-171 and to communicate directly to DoD as required. Govaged, Inc. will need to be kept informed of any compliance or incident issues as follows:

Provide a copy of any DoD NIST compliance reports as well as any deficiency communications to the Govaged, Inc. Procurement representative identified on any associated purchase order or contract.

For any incidents (as defined by 252.204-7012) of CUI or Govaged, Inc. sensitive data, notify the Procurement representative identified on any associated purchase order or contract for which the incident occurred with 72 hours of discovery.

USA: 4517 La Salle Ave, Alexandria VA 22304-1524
UK: 208 Pill Box Studios, 115 Coventry Road, London E2 6GG England
Ph.: 1.302.257.2327 | Fax: 1.302.450.1920
| Ph.: 1.302.608.0208
www.govaged.com | www.govaged.co.uk

ADDITIONAL CYBERSECURITY RESOURCES:

There are many IT securities related resources to provide awareness and to help improve your security program. There are also many security organizations that provide guidance on cyber threats as well as methods to assess and mitigate cyber risks. Govaged, Inc. does not endorse any specific resource or organization and provides this information as a courtesy to suppliers that may not be aware of some of the resources available.

CIS (Center for Internet Security)

ISO (International Organization for Standardization)

NIST (National Institute of Standards and Technology)

SANS Institute

US-Cert

USA: 4517 La Salle Ave, Alexandria VA 22304-1524
UK: 208 Pill Box Studios, 115 Coventry Road, London E2 6GG England
Ph.: 1.302.257.2327 | Fax: 1.302.450.1920
| Ph.: 1.302.608.0208
www.govaged.com | www.govaged.co.uk