Cybersecurity Compliance is Mandatory

Manufacturers doing business directly or indirectly for the DoD, GSA, and NASA must meet Defense Federal Acquisition Regulation (DFAR) minimum cybersecurity standards or risk losing contacts. Compliance is an on-going process so don't delay.

CONNSTEP works in collaboration with manufacturers and their IT resources to improve the safeguards of defense-related data and ensures your compliance with the controls described in NIST Special Publication 800-171.

CONNSTEP can help you manage your cybersecurity risk and ensure the integrity of your defense-related data. Contact us today.

Our services include a methodical approach that includes:

Executive Overview of DFARS Compliance and NIST SP 800-171

- Steps and processes required to achieve compliance over time and other related federal cyber regulations

Gap Analysis

- Evaluate security controls, identify gaps with respect to NIST SP 800-171, and develop recommendations for improvements in a Plan of Action with Milestones (POAM)

Cybersecurity Maturity Model Certification (CMMC)

- Review areas of CMMC requirements that may apply to your business so that you can start planning now

Customized Plan Development

- **System Security Plan:** based on the current state of your system with input from your IT resources, also contributes to CMMC preparation
- **Incident Response Plan:** to help detect, respond to, and recover from network security issues
- **Policy and Procedures**: documentation designed to meet NIST SP 800-171 standards and train employees on them

Cyber Security Evaluation Tool (CSET®)

- CSET is a software package from the Department of Homeland Security that provides a systematic and repeatable approach for assessing the security posture of your cyber systems and networks

CONNSTEP
a CBIA affiliate

connstep.org | 800.266.6672