

CONTROLLED UNCLASSIFIED INFORMATION

DFARS/FAR COMPLIANCE

CUI Contractor Certification DFARS/FAR Compliance Requirements

Do not risk losing federal business and government contracts by not being compliant with the security requirements identified in NIST SP 800-171. FAR 52.204-21 and DFARS 252.204-7012 require contractors to ensure the security and confidentiality of Controlled Unclassified Information (CUI) and Covered Defense Information (CDI). COACT can reduce the time and resources needed to demonstrate compliance.

OVERVIEW

NIST SP 800-171 prescribes security requirements for Federal agencies to safeguard CUI that resides outside of agency control.

Nonfederal organizations are required to comply with CUI security requirements:

1. When CUI is resident in a nonfederal system/organization;
2. When the nonfederal organization is NOT collecting or maintaining CUI on behalf of the government or using/operating a system on behalf of the government; and
3. When there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by any law, regulation, or governmentwide policy.

CUI basic and derived security requirements apply to all components of nonfederal information systems and organizations that process, store, and/or transmit CUI.

Subcontractors that process, store, and/or transmit CUI and external third-party providers of security protection services for CUI components must also comply.

COACT METHODOLOGY



SCOPING

COACT evaluates the security posture of information systems that process, store, and/or transmit CUI. Activities focus on documentation development and review, definition of system boundary, and an evaluation of policies and procedures.



REQUIREMENTS

COACT ensures that nonfederal organizations implement controls and document implementations to satisfy the security requirements in NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.



ASSESSMENT

COACT assesses the implementation of requirements in accordance with NIST SP 800-171A to demonstrate systems, facilities, and procedures in place to safeguard CUI consistent with security guidelines defined in NIST SP 800-171.



MONITOR

COACT ensures compliance by developing a continuous monitoring strategy to periodically assess a subset of the security requirements and monitor security control effectiveness.

COACT, Inc. is a Service Disabled Veteran Owned Small Business (SDVOSB) and a FedRAMP accredited Third Party Assessment Organization (3PAO), which was founded in 1990. For over 25 years, COACT has been providing consulting, Independent Verification and Validation (IV&V), and documentation development services to both government and commercial clients to guide them in understanding and fulfilling their risk management and compliance needs.

MAKE DECISIONS WITH IMPACT

Why Choose COACT?

ACCREDITED 3PAO

Accredited by the American Association for Laboratory Accreditation (A2LA) as a Federal Risk Authorization Management Program (FedRAMP) Third Party Assessment Organization (3PAO). A2LA evaluated the technical competence of COACT and compliance with international standards including: ISO/IEC 17020:2012 and ISO 9001:2015.

TECHNICAL EXPERTISE

COACT has over 25 years of experience in providing Independent Verification and Validation (IV&V) services to both commercial and government clients. COACT's knowledge of various compliance frameworks can assist covered contractors in evaluating security safeguards to meet the CUI requirements associated with the appropriate category or subcategory.

INDEPENDENCE

COACT ensures the performance of impartial assessments and provides objective recommendations associated with remediation of findings. COACT will not represent a mutual or conflicting interest with your organization, act as management or personnel, or place ourselves in positions of advocacy for your organization.

QUALITY

COACT can streamline the CUI (i.e. FAR/DFARS) compliance process using an accredited Quality System to meet customer requirements and improve the security posture of systems, facilities, and procedures.

OUR SERVICES

KICKOFF

Presentation and discussion regarding CUI security requirements, CUI category/subcategory designation, secure architecture design, and assessment methodology.

ASSESSMENT

Perform an assessment in accordance with a Security Assessment Plan (SAP) developed using NIST SP 800-171A. A Security Assessment Report (SAR) is generated that describes the level of compliance and identifies evidence that satisfies the applicable basic and derived CUI security requirements.

MONITOR

Assist Covered Contractors in maintaining compliance by developing assessment strategies to ensure compliance to CUI security requirements and streamline authorization efforts.

CONSULT

Provide consulting and advisory services to guide organizations through the process of satisfying basic and derived CUI security requirements by driving documentation development and remediation efforts.

- 📍 9140 Guilford Road, Suite N, Columbia MD 21046
- ✉ info@coact.com
- 🌐 www.coact.com
- ☎ 301.498.0150