COALFIRE

DATASHEET

DFARS / NIST SP 800-171 compliance services

Meet Department of Defense Contracting Requirements

Maintain government contract award eligibility by demonstrating compliance with NIST SP 800-171 for Department of Defense (DoD) Federal Acquisition Regulations Supplement (DFARS) requirements. Federal government mandates and NIST SP 800-171 compliance can be time consuming and confusing for your internal staff. Coalfire's NIST-based compliance service takes the burden off you so you can continue doing business as usual.

BACKGROUND

- NIST SP 800-171 states that nonfederal contractors or subcontractors that collect, store, or transmit covered defense information (CDI) or controlled unclassified information (CUI) on nonfederal systems to the federal government will need to comply with NIST SP 800-171 by December 31, 2017 or risk losing government contracts. All prime contractors and their subcontractors must comply.
- The DoD has updated the DFARS, requiring contractors to be compliant with NIST SP 800-171 "as soon as practical, but no later than December 31, 2017" (252.204-7012.ii.A).
- DFARS clause 252.204-7008 addresses requirements for safeguarding CDI controls in government contractor systems, which include CDI and CUI. Clause 252.204-7012 addresses the expansion of safeguards to include cyber incident reporting requirements.

DFARS / NIST 800-171 SERVICES: WHAT'S INCLUDED?

Coalfire's experience with NIST SP 800-171 and other NIST-based assessments can be applied to your organization in the following methods:

- **Workshop:** One- to two-day, onsite, presentation and discussion on NIST 800-171 requirements, compliance process, and current technical capabilities.
- **Gap analysis:** Coalfire's advisory team will conduct a compliance analysis of current information systems against NIST SP 800-171. Findings include current compliance posture, identification and verification of organization security boundaries, system policies and procedures status, and roadmap for DFARS/NIST SP 800-171 compliance.
- **Advisory:** Coalfire's advisory team will assist in the design and documentation development of the system security plan (SSP) and several closely associated supporting documents that are required to achieve DFARS compliance. Coalfire will also provide DFARS reference architecture recommendations and engineering roadmap considerations.
- **Assessment:** Coalfire can develop and test against a DFARS security assessment plan (SAP) that includes NIST SP 800-171 controls. The assessment report will indicate the compliance posture with DFARS.
- **Compliance automation dashboard:** For companies leveraging a security and monitoring analytics tool (e.g., Splunk), Coalfire can provide engineering services to implement and help automate controls for NIST SP 800-171 compliance for a single pane view of your compliance status in real time.

COALFIRE DIFFERENCE

Save time and resources
Identify gaps and streamline your NIST 800-171 compliance efforts by working with experienced assessors who have an in-depth understanding of your industry and technology.

Requirement clarity
Coalfire will provide clarity for the NIST 800-171 compliance requirements and guidance on how to mitigate deficiencies.

Tailored approach based on deep technical expertise
Coalfire has 16 years of experience in NIST-based compliance that is relied on by leading agencies such as HHS, CMS, NIH, DHS, DOT, and many more. Coalfire's expertise is directly drawn from working with several thousands of NIST-based gap assessments, advisory, and assessment projects across multiple industries. With this depth of experience and knowledge, Coalfire can help you understand your security posture and how it compares to your industry peers.

Independent advice
Coalfire's firm stance on technology and vendor independence allows for thorough in-depth and unbiased recommendations from an experienced third party. Our services will provide an objective and knowledgeable view of how the requirements that affect your organization.

Coalfire's process

Coalfire will rely on our understanding of NIST assessments and other published guidance (agency supplied) to evaluate the required controls against the existing implementations presented by client stakeholders. Our approach covers the subset of NIST 800-171 controls to include:

- Access controls
- Awareness and training
- Audit and accountability
- Configuration management
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Personnel security
- Physical protection
- Risk assessment
- Security assessment
- System and communications protection
- System and information integrity

The outcome will provide you with a thorough understanding of compliance with NIST 800-171, as well as a clear articulation of any gaps, which will need to be addressed following completion of the engagement for your organization to be in full compliance with NIST 800-171.

Coalfire's experience
While NIST 800-171 is a relatively new compliance requirement, Coalfire has conducted 800-171 engagements for both large enterprise service providers and original equipment manufacturers, as well as small/mid-size businesses working with the United States federal government.

DS_DFARSNIST_081117

COALFIRE

About Coalfire
Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. **Coalfire.com**