TEVORA

tevora.com

Solution Services

DFARS Compliance

The Defense Federal Acquisition Regulation Supplement (DFARS) lays out cybersecurity requirements for Department of Defense (DoD) contractors, including requirements for protecting information as specified in the National Institute of Standards and Technology (NIST) Special Publication 800-171. These requirements also apply to companies that supply goods or services to DoD contractors.

If you are seeking a new contract for goods or services that will be sold to the DoD, you'll need to demonstrate compliance with DFARS/NIST 800-171, and failure to maintain compliance can be grounds for contract termination.

The good news is that our team of expert consultants can help you navigate these complex requirements and attain full compliance.

Tevora is an accredited Cybersecurity Inspector for conducting NIST 800-171 services. We have perfected our program for helping clients achieve compliance through years of working as a security advisor to some of the largest companies in the world.

Let Tevora be a trusted partner to help you plan for and attain DFARS compliance.

How Tevora Helps You Comply with DFARS

1. **Gap Analysis**—Our expert consultants work with your team to identify areas where you are not yet in compliance with DFARS/NIST 800-171 requirements.
2. **Remediation Support**—Our team partners with you to develop and implement plans to address the technology, policy, process, training, and other gaps that you need to close to achieve DFARS/NIST 800-171 compliance.
3. **DFARS Assessment**—After the gaps have been closed, we leverage our skills as an accredited NIST 800-171 Cybersecurity Inspector to validate that you are fully compliant. After successful validation, we'll provide you with documentation that demonstrates your compliance to the DoD.

TEVORA

tevora.com

Our Purpose

To protect the world from cyberthreats.

Insightful Advice
Expert Resource
Confident Delivery

About Us

Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Irvine, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's digital assets. We make it our responsibility to ensure the CISO has the tools and guidance they need to build their departments, so they can prevent and respond to daily threats.

Our expert advisors take the time to learn about each organization's unique pressures and challenges, so we can help identify and execute the best solutions for each case. We take a hands-on approach to each new partnership, and—year after year—apply our cumulative learnings to continually strengthen the company's digital defenses.

Go forward.
We've got your back.

DFARS Background

The federal government established DFARS in 2012 to address the need for its contractors to provide assurance that Covered Defense Information (CDI), Controlled Unclassified Information (CUI), and Controlled Technical Information (CTI) are being protected in a manner commensurate with their respective sensitivity.

This can include the following types of data:

- Critical Infrastructure
- Defense
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- NATO
- Nuclear
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional
- Statistical
- Tax

Tevora's Expert Team

Our experienced and knowledgeable security team has a proven track record helping clients gain an in-depth understanding of the data they get or hold from the DoD—including all the types listed above. We can help you take the appropriate steps to properly protect each type of data in accordance with DFARS/NIST 800-171 requirements.

We would welcome the opportunity to partner with you to untangle the mysteries of DFARS and help you achieve full compliance.

HITRUST Authorized CSF Assessor