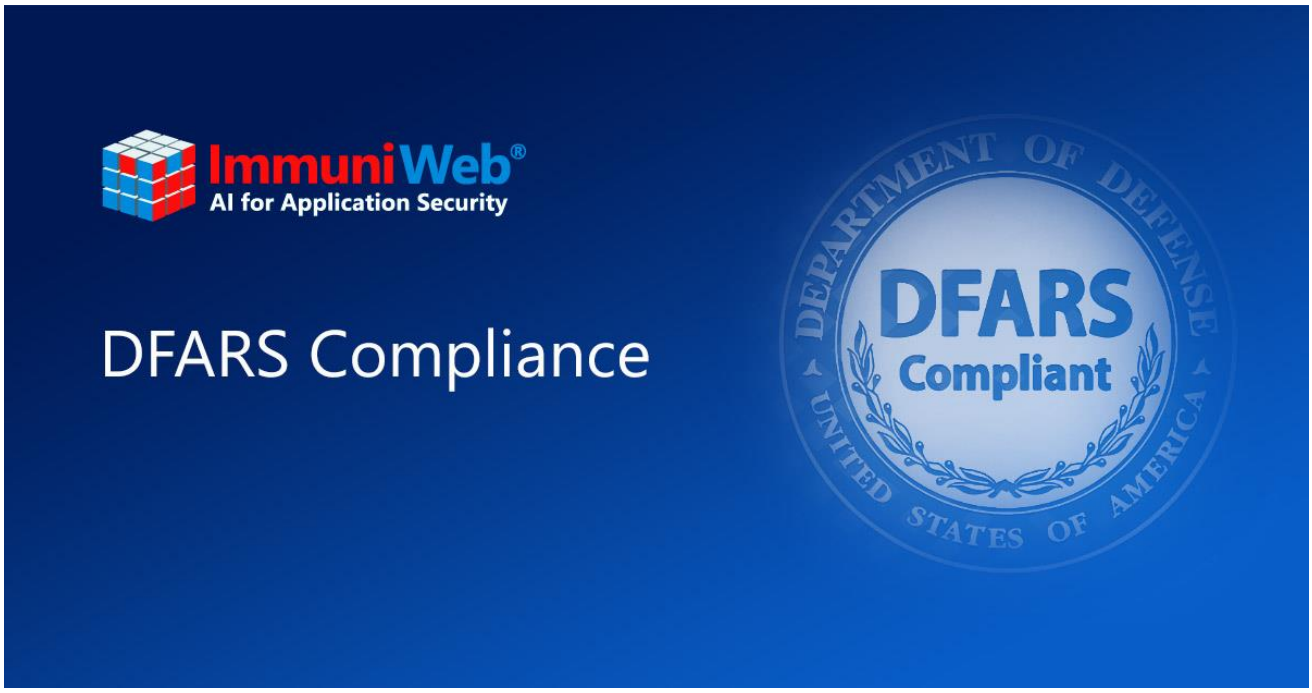
DFARS Compliance

DFARS Compliance: A Brief Overview



DFARS (Defense Federal Acquisition Regulations Supplement) is a set of regulations that govern the acquisition of goods and services by the U.S. Department of Defense. It includes specific requirements related to the protection of national security information.

Key DFARS Requirements for Protecting National Security Information:

- Cybersecurity: DFARS requires contractors to implement cybersecurity measures to protect national security information. This includes conducting risk assessments, developing incident response plans, and implementing security controls.
- Controlled Unclassified Information (CUI): DFARS defines CUI as information that is not classified but requires protection from unauthorized disclosure. Contractors must implement controls to protect CUI.
- Data at Rest: DFARS requires contractors to protect data at rest, including both classified and unclassified information. This involves encrypting data and implementing access controls.

- Data in Transit: DFARS requires contractors to protect data in transit, such as when data is being transmitted over networks. This involves using encryption and other security measures.
- Subcontractors: DFARS requires contractors to ensure that their subcontractors also comply with DFARS requirements for protecting national security information.

Consequences of Non-Compliance:

Failure to comply with DFARS can result in significant consequences, including:

- Termination of Contracts: The government may terminate contracts with non-compliant contractors.
- Fines and Penalties: Contractors may be subject to fines and penalties for violations of DFARS.
- Damage to Reputation: Non-compliance can damage a company's reputation and make it difficult to obtain future government contracts.

Tips for DFARS Compliance:

- Conduct a Risk Assessment: Conduct a thorough risk assessment to identify potential vulnerabilities in your systems and data.
- Develop a Security Plan: Develop a comprehensive security plan that addresses all DFARS requirements.
- Implement Security Controls: Implement appropriate security controls to protect national security information.
- Train Employees: Train employees on how to recognize and report potential security threats.
- Monitor and Review: Regularly monitor and review your security measures to ensure that they remain effective.

Learn more about CFAA compilance.

What's Next?

- ✓ Learn more about ImmuniWeb Compliance Services.
- ✓ Read ImmuniWeb Cyber Law and Cybercrime Investigation Blog.
- ✓ Join ImmuniWeb at the upcoming Webinars and Events.
- ✓ Follow ImmuniWeb on LinkedIn, X (Twitter), and Telegram.
- ✓ Subscribe to ImmuniWeb Newsletter.
- ✓ Try ImmuniWeb Community Edition Free Security Tests.
- ✓ See the benefits of ImmuniWeb Partner Program.

ImmuniWeb® AI for Application Security

The award-winning ImmuniWeb® AI Platform helps over 1,000 customers from over 50 countries to test, secure and protect their web and mobile applications, cloud and network infrastructure, to prevent supply chain attacks and data breaches, and to comply with regulatory requirements.

- API Penetration Testing
- Continuous Automated Red Teaming
- Dark Web Monitoring
- Phishing Websites Takedown
- API Security Scanning
- Continuous Breach and Attack Simulation
- Digital Brand Protection
- Red Teaming Exercise