How CrashPlan Helps Organizations Maintain DFARS Compliance

CrashPlan

TECH OVERVIEW

CrashPlan supports customer compliance with Defense Federal Acquisition Regulations Supplement (DFARS) requirements, giving organizations the critical data backup and recovery and confidentiality capabilities needed for safeguarding Covered Defense Information (CDI). In addition, CrashPlan provides a powerful data protection foundation that contributes to a long-term DFARS compliance strategy and prepares organizations to meet evolving regulations and complex compliance requirements.

What is DFARS?

DFARS clause 252.204-7012 was structured to ensure that unclassified DoD information residing on a contractor's internal information system is safeguarded from cyber incidents, and that any consequences associated with the loss of this information are assessed and minimized via the cyber incident reporting and damage assessment processes.

CrashPlan and DFARS

UNDER DFARS, DOD CONTRACTORS AND SUB-CONTRACTORS WHO POSSESS, STORE OR TRANSMIT COVERED DEFENSE INFORMATION (CDI) MUST:

- **Comply with the security requirements in NIST 800-171**
- **Address the safeguarding of CDI**
- **Report cyber incidents involving CDI**
- **Report any cyber incident that may affect the ability to provide operationally critical support**

As a data protection for backup and recovery solution that has the potential to store CDI, CrashPlan complies with DFARS baseline security standards.

Data Encryption in CrashPlan

CrashPlan doesn't have to deploy a specialized solution for customers that fall under DFARS. That's because we protect customer data with end-to-end encryption: 256-bit AES to secure data at rest and 256-bit Transport Layer Security (TLS) 1.2 encryption to secure all data in transit, utilizing FIPS 140-2 validated modules.

Information System Security

Central to protection of CDI from cyber incidents, contractors and subcontractors must also provide adequate security for all CDI. CrashPlan has dedicated security staff supporting CrashPlan and its environments.

NIST 800-171

CrashPlan meets applicable security requirements equivalent to those established by the Government for NIST

800-171 in our product and internal network environments. For details on how CrashPlan meets the applicable NIST 800-171 controls, please contact your CrashPlan representative.

CYBER INCIDENT RESPONSE

A key component of DFARS is the ability for contractors and subcontractors to investigate, respond and recover to potential or actual compromises of CDI. CrashPlan has a robust incident response program that complies with the DFARS cyber incident reporting requirements, including:

- **Cyber incident investigation capabilities**
- **Prompt reporting (within 72 hours of discovery) of cyber incidents**
- **Ability to identify, isolate, and provide a copy of malicious software, as applicable to the incident**
- **Ability to preserve, protect and recover images of impacted systems**
- **Access to covered contractor information systems and other information, as required by DoD**

At CrashPlan, we believe DFARS compliance is about more than checking boxes; it's about choosing solutions that enable your organization to mitigate the risk of CDI being lost. With CrashPlan you have the ability to protect, backup and recover from any data loss event.

For most of today's businesses, your data IS your business. CrashPlan features protect your data from natural disasters, ransomware attacks, coffee spills, and even that employee that quits and deletes the team folder on the way out.

CrashPlan Answers the Big DFARS Questions

CrashPlan plays a vital role in helping a wide range of organizations secure, backup and recover their CDI while maintaining DFARS compliance.

DOES CRASHPLAN COMPLY WITH NIST 800-171?

Yes. CrashPlan either directly meets the defined controls, provides compensating controls offering similar or greater assurance, or accepts risk for controls that aren't applicable to our environment.

CAN CRASHPLAN MEET THE CYBER INCIDENT REPORTING REQUIREMENTS?

Yes. CrashPlan has a robust incident response program that complies with the DFARS cyber incident reporting and recovery requirements and has a DoD approved medium assurance certificate to report cyber incidents.

WILL OUR DOD DATA RESIDE IN THE U.S.?

Yes. CrashPlan offers the flexibility to choose where your data will reside so organizations can build a solution that fits their data security and compliance needs. With our agile cloud platform, CrashPlan customers can elect to keep all data at cloud storage locations within the U.S.

CrashPlan

Corporate Headquarters
400 S 4th St Suite 410
PMB 31083
Minneapolis, MN 55415-1419
612.464.2112

crashplan.com

CrashPlan® provides peace of mind through secure, scalable, and straightforward endpoint data backup. We help organizations recover from any worst-case scenario, whether it is a disaster, simple human error, a stolen laptop, ransomware or an as-of-yet undiscovered calamity. We continue to innovate as the landscape of work evolves, which makes CrashPlan foundational to organizations' data security. What starts as endpoint backup and recovery becomes a solution for ransomware recovery, breaches, migrations, and legal holds.

For more information, visit **crashplan.com**.