code42

How Does Code42's Incydr Gov Help Organizations Maintain DFARS Compliance

Our Insider Risk Management solution, Incydr supports customer compliance with Defense Federal Acquisition Regulations Supplement (DFARS) requirements, giving organizations the critical data risk detection and response capabilities needed for safeguarding Covered Defense Information (CDI). In addition, Incydr 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.

Code42 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 insider risk solution that has the potential to store CDI, Code42 complies with DFARS baseline security standards.

Data encryption in Incydr

Incydr 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.

Information system security

Central to protection of CDI from cyber incidents, contractors and subcontractors must also provide adequate security for all CDI. Incydr is an ISO 27001 certified organization with a dedicated security staff supporting Incydr and its cloud environments.

NIST 800-171

Incydr meets applicable security requirements equivalent to those established by the Government for NIST 800-171 in our Incydr product and internal network environments. For details on how Incydr meets the applicable NIST 800-171 controls, please contact your Incydr representative.

Cyber incident response

A key component of DFARS is the ability for contractors and subcontractors to investigate and respond to potential or actual compromises of CDI. Incydr 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 and protect images of impacted systems
- Access to covered contractor information systems and other information, as required by DoD

At Code42, 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 falling into the wrong hands. With Incydr you have the ability to detect, mitigate and respond to data exfiltration and insider risks.

See how your employees move data across vectors—including web browser uploads, cloud sync activity, cloud file sharing, email, and use of removable media. Leverage this powerful data visibility to enable a proactive and intelligent approach to data security and protection. Establish baselines of normal individual user behavior and detect deviations or unusual activity. In short, spot anomalies sooner. Take action faster.

Incydr answers the big DFARS questions

Incydr solutions play a vital role in helping a wide range of organizations secure and control their CDI while maintaining DFARS compliance.

Does Incydr comply with NIST 800-171?

Yes. Incydr 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 Incydr meet the cyber incident reporting requirements?

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

Will our DoD data reside in the U.S.?

Yes. Incydr 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, Incydr customers can elect to keep all data at cloud storage locations within the U.S.

About Code42

Code42 is the leader in Insider Risk Management. Native to the cloud, the Code42® Incydr™ solution rapidly detects data loss and speeds incident response without inhibiting employee productivity. With Code42, security professionals can protect corporate data and reduce insider threats while fostering an open and collaborative culture for employees. More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. For more information, visit **code42.com**.