The Requirement

- Controlled Unclassified Information (CUI) is non-classified information that is shared by the federal government with a nonfederal entity. CUI requires security protection when processed, stored, transmitted and used in nonfederal information systems. The requirements to protect CUI are outlined in NIST 800-171.
- NIST 800-171 requirements are based on NIST 800-53 Moderate baseline.

When does it apply?

- Direct reference to NIST 800-171
- 32 CFR 2002 Controlled Unclassified Information
- DFARS 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct 2016)
- 252.204-7000 Disclosure of Information (Oct 2016)
- 52.204-21 Basic Safeguarding of Contractor Information

The Solution

Sherlock Cloud - A multi-tenant, scalable, managed, Cloud platform built according to NIST 800-53 requirements to comprehensively address the CUI requirements.

Sherlock Cloud has expanded its compliance expertise to offer solutions utilizing the AWS or Azure Cloud. Sherlock customers have the option to choose managed CUI-compliant services operating on premise at SDSC, in the AWS Cloud, or in Azure Cloud.

Examples of Sherlock Cloud controls that apply to CUI

- System maintenance (timely patch/flaw redemption)
- Central log collection and review of system logs
- Intrusion Detection Systems (IDS) monitoring, analysis and reporting
- Strong authentication using two factor, one-time tokens
- Protection of data-at-rest through encryption (FIPS 140-2)
- Hardened system configurations (STIG and CIS)
- Use of jump-boxes to isolate systems and limit system exposure
- Encrypted tunnels for data-in-transit outside of private network (SSH, RDP, SSL)
- Web proxies and filters to limit web access
- Host-based firewalls
- Malicious software protection (Anti-Virus/Anti-Malware)