

# Are You in Compliance?

## Guidance on CUI in the National Institute of Standards and Technology (NIST) SP 800-171 Revision 3

Outlined below are some key takeaways from the draft guidance on CUI in NIST SP 800-171 Rev. 3, and ways SyberGRC can assist in achieving compliance.



### Audit Information Access (R3-03-03-09)

Authorize access to management of audit logging and information, including static data relevant to applicable audits.

**How We Help:**

iDPS can be implemented alongside dedicated personnel to ensure the **periodic assessments across your network** are being conducted with the appropriate resources, while achieving ultimate data awareness in respect to any upcoming, pending, or ongoing audits.



### Media Storage (R3-03-08-01)

Entities are required to be aware of, control, and securely store digital and non-digital media containing CUI until the media are destroyed or sanitized.

**How We Help:**

iDPS will provide the **location of sensitive data across all the assets** your organization requires oversight on. Understanding the content and location of the data, CUI, and media will achieve compliance in both storage and disposal requirements.



### Information in Shared System Resources (R3-03-13-04)

Unauthorized and unintended information transfer between shared system resources must be prevented.

**How We Help:**

By using iDPS across shared system resources and assets, existing static data can be located and identified **before or after it has been transferred**, which assists in compliance with requirements



### Transmission and Storage Confidentiality (R3-03-13-08)

Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.

**How We Help:**

In addition to locating applicable CUI and sensitive data, iDPS will **identify files that already contain permissions** and can help in verifying the appropriate access and storage is applied to each individual file.



### Protection of Audit Information (R3-03-03-08)

Protect audit information and audit logging tools from unauthorized access, modification, and deletion

**How We Help:**

iDPS classifies and locates all sensitive data across your business using **customized keywords that are critical to your operations and industry**. Unstructured audit and CUI data can be used as the basis of an iDPS implementation, and thus protected once discovered.

## Contact Us

<https://www.sybergrc.com>

908-510-3531