FORTRA

NIST Regulations For Controlled Unclassified Information (CUI)

CUI And NIST At A Glance

Classifying and Controlling Government Data in Nonfederal Systems

Organizations that work with U.S. government agencies, or want to compete to do so, must meet new data handling procedures. In December 2017, the **National Institute of Standards and Technology (NIST) Special Publication 800-171 standards and guidelines** were introduced, regulating the management of government data while residing in, processed by or traversing through nonfederal information systems.

Known as Controlled Unclassified Information (CUI), this information is used by nonfederal external service providers to perform a wide range of business functions not typically suited for government agencies. These external service providers bring to bear state of the art technologies, capabilities and resources that would otherwise not be available to the government in the execution of their missions.

Government bodies, their commercial contractors and subcontractors must maintain compliance with NIST SP800-171 standards and guidelines throughout the contract's lifecycle where CUI is involved. To ensure this, all documents, drawings and emails containing CUI must be appropriately marked, and marking must clearly be visible in the header and footer of documents.

The Executive Agent (EA) has created and manages a publically available CUI registry, which specifies, by category and subcategory, which marking must be applied to a particular data subject. The registry also details procedures relating to the handling, safeguarding and control of the data as it moves through nonfederal systems. The marking is central to ensuring that CUI data is handled and secured in an appropriate way, and is only accessible to users who need to work with it, such as for a particular project.

What Is CUI?
Controlled Unclassified Information which isn't classified by Executive Order 13526, or the Atomic Energy Act that should not be made public as a result of law, regulations, or government-wide policies

What Defines How CUI Should Be Controlled?
National Institute of Standards and Technology (NIST) Special Publication 800-171 as stipulated by DFARS 252.204-7012

How Do I Find The Correct Marking For CUI?
The Executive Agent (EA) public registry of categories, subcategories, and CUI corresponding CUI markings, on the NARA website

NIST SP800-171 standards and guidelines require a security plan be developed and maintained for CUI data, covering a range of issues including access control, audit and accountability and system and information integrity. This must consist of technical security and compliance documentation consistent with 14 security control families:

1. Access Control

2. Awareness and Training

3. Audit and Accountability

4. Configuration Management

5. Identification and Authentication

6. Incident Response

7. Maintenance

8. Media Protection

9. Personal Security

10. Physical Security

11. Risk Assessment

12. Security Assessment

13. System Communication & Protection

14. System and Information Integrity

Boldon James Classifier can help organizations in applying and managing CUI marking in order to meet NIST standards and guidelines. The Classifier range can apply user-driven and automated classification markings over a market leading range of applications, embedding CUI marking into an organization's federal contracting processes. As well as applying the visual markings required for CUI, Classifier applies persistent file metadata, ensuring that it remains securely in the DNA of the document or file. Classifier can also drive rules governing the dissemination (malicious and accidental) and storage of protected data. The Classifier reporting suite enables organizations to demonstrate this compliance, helping you to show your organization's readiness to manage government contracts involving CUI data.

How Can Boldon James Help?

Boldon James Classifier, the market leading data classification product, supports compliance with NIST regulations by:

- Apply CUI visual markings and metadata to documents and files over a market-leading range of applications

- Adjustable categories and subcategories that can be tailored to specifically match the CUI marking needs of your organization

- Protecting users and organizations from accidental or malicious dissemination of CUI information

- Clear, persistent marking of documents and files while at rest or in transit

- Intelligent integrations with complementary best-of-breed security controls in areas such as discovery, DLP, CASB, encryption, archival and rights management

- Enabling bulk classification to ensure all files in a project can be marked appropriately to meet the CUI marking rules with speed and simplicity

- Helping to demonstrate compliance with a comprehensive reporting capability or through inclusion with 3rd party reporting solutions (e.g. SIEM)

Don't Delay Your Preparations

The standardization of markings brought about by the NIST standards and guidelines offers organizations the opportunity to demonstrate their ability to operate as a trusted partner to government. Implementing a classification solution, such as Boldon James Classifier, now illustrates your preparedness to manage CUI, empowering your organization in the competition for government contracts.

Visit boldonjames.com/NIST for more information on how data classification can protect your sensitive data.

FORTRA

Fortra.com